

IBM WebSphere Application Server for z/OS, Version 8.5

*Installing your application serving
environment*



Note

Before using this information, be sure to read the general information under “Notices” on page 569.

Compilation date: May 14, 2012

© Copyright IBM Corporation 2012.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

How to send your comments	vii
Using this PDF	ix
Chapter 1. What is new for installers	1
Chapter 2. How do I install an application serving environment?	3
Chapter 3. Task overview: Installing on z/OS	5
WebSphere Application Server Version 8.5 product offerings for supported operating systems	5
Directory conventions	15
Hardware and software requirements on z/OS	15
z/OS driving system requirements	16
z/OS target system requirements	16
Skill requirements	18
Creating implementation plans on z/OS	18
Product file system	20
Chapter 4. Planning for product installation	23
Chapter 5. Installing the product on z/OS	27
Obtaining an Installation Manager installation kit for installing the product on z/OS	27
Creating an Installation Manager for installing the product on z/OS	28
Obtaining product repositories for installing the product on z/OS	31
Installing WebSphere Application Server for z/OS	33
Installing IBM WebSphere SDK Java Technology Edition Version 7.0	36
Installing DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS	37
Installing Web Server Plug-ins for IBM WebSphere Application Server for z/OS	39
Chapter 6. Installing and using the WebSphere Customization Toolbox	43
Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox	44
Installing the WebSphere Customization Toolbox using the GUI	45
Installing the WebSphere Customization Toolbox using response files	49
Installing the WebSphere Customization Toolbox using the command line	55
Installing and removing tools in the WebSphere Customization Toolbox	59
Installing fix packs on the WebSphere Customization Toolbox using the GUI	61
Uninstalling fix packs from the WebSphere Customization Toolbox using the GUI	62
Uninstalling the WebSphere Customization Toolbox using the GUI	62
Uninstalling the WebSphere Customization Toolbox using response files	63
Uninstalling the WebSphere Customization Toolbox using the command line	65
Chapter 7. Preparing the base z/OS operating system	67
Preparing z/OS to run WebSphere Application Server	68
Preparing the sysplex on z/OS	69
Preparing JES2 or JES3	70
Preparing Resource Recovery Services (RRS)	71
Preparing the security server (RACF)	72
Preparing TCP/IP on z/OS	73
Checklist: Preparing the base z/OS operating system	75
Chapter 8. Planning for product configuration on z/OS	77
WebSphere Application Server for z/OS terminology	78
Using a heterogeneous cell to support mixed platforms within a cell	82

Considerations for WebSphere Application Server for z/OS	82
z/OS JCL cataloged procedures	82
Configuration file systems	86
z/OS logstreams	90
Output destinations	93
Reusable address space	93
Scheduler database	94
Port number settings on z/OS	95
z/OS workload management (WLM).	99
Standalone and Network Deployment configuration differences.	99
z/OS application server naming conventions	99
z/OS basic naming convention	101
z/OS standard naming convention	107
Configuration Planning Spreadsheets for z/OS	111
Default port assignments	111
Initial security configurations	113
Building practice WebSphere Application Server for z/OS cells	115
Planning for standalone application server cells	117
z/OS customization variables: Standalone application servers	118
z/OS customization worksheet: Standalone application servers for Version 7.0	133
z/OS customization worksheet: Standalone application servers for Version 8.0	142
z/OS customization worksheet: Standalone application servers for Version 8.5	151
Planning for administrative agents	159
z/OS customization variables: Administrative agents	160
z/OS customization worksheet: Administrative agents for Version 7.0	173
z/OS customization worksheet: Administrative agents for Version 8.0	180
z/OS customization worksheet: Administrative agents for Version 8.5	187
Planning for deployment managers	194
z/OS customization variables: Deployment managers	194
z/OS customization worksheet: Deployment managers for Version 7.0	207
z/OS customization worksheet: Deployment managers for Version 8.0	214
z/OS customization worksheet: Deployment managers for Version 8.5	221
Planning for new managed (custom) nodes	228
z/OS customization variables: Managed (custom) nodes.	229
z/OS customization worksheet: Managed (custom) nodes for Version 7.0	242
z/OS customization worksheet: Managed (custom) nodes for Version 8.0	249
z/OS customization worksheet: Managed (custom) nodes for Version 8.5	256
Planning to federate standalone servers into a Network Deployment cells	264
z/OS customization variables: Federating application servers	264
z/OS customization worksheet: Federating application servers for Version 7.0.	269
z/OS customization worksheet: Federating application servers for Version 8.0.	271
z/OS customization worksheet: Federating application servers for Version 8.5.	273
Planning for Network Deployment cells with application servers	276
z/OS customization variables: Network Deployment cells with application servers	276
z/OS customization worksheet: Network Deployment cells with application servers for Version 7.0	295
z/OS customization worksheet: Network Deployment cells with application servers for Version 8.0	304
z/OS customization worksheet: Network Deployment cells with application servers for Version 8.5	314
Planning for job managers.	324
z/OS customization variables: Job managers	324
z/OS customization worksheet: Job managers for Version 7.0.	337
z/OS customization worksheet: Job managers for Version 8.0.	344
z/OS customization worksheet: Job managers for Version 8.5.	351
Planning for secure proxy servers	358
z/OS customization variables: Secure proxy servers	358
z/OS customization worksheet: Secure proxy servers for Version 7.0	369
z/OS customization worksheet: Secure proxy servers for Version 8.0	376

z/OS customization worksheet: Secure proxy servers for Version 8.5	382
Planning for secure proxy administrative agents	387
z/OS customization variables: Secure proxy administrative agents	389
z/OS customization worksheet: Secure proxy administrative agents for Version 7.0	400
z/OS customization worksheet: Secure proxy administrative agents for Version 8.0	407
z/OS customization worksheet: Secure proxy administrative agents for Version 8.5	413
Planning for recovery	420
Starting deployment managers on a different MVS image	420
Automatic restart management (ARM)	421
Problem diagnostic plan strategy	425
Chapter 9. Configuring the WebSphere Application Server for z/OS product after installation	427
Configuring z/OS application-serving environments with the Profile Management Tool (z/OS only)	427
Using the Profile Management Tool (z/OS only)	429
Creating standalone application server cells on z/OS using the Profile Management Tool.	436
Creating administrative agents on z/OS using the Profile Management Tool	436
Creating deployment managers on z/OS using the Profile Management Tool	437
Creating managed nodes on z/OS using the Profile Management Tool	440
Federating standalone application servers into Network Deployment cells on z/OS using the Profile Management Tool	442
Creating Network Deployment cells with application servers on z/OS using the Profile Management Tool	443
Creating job managers on z/OS using the Profile Management Tool	444
Creating secure proxy servers on z/OS using the Profile Management Tool.	445
Creating secure proxy administrative agents on z/OS using the Profile Management Tool	445
Configuring with symbolic links on z/OS.	446
Configuring z/OS application-serving environments with the zpmt command	446
zpmt command	448
Variables for configuring standalone application servers using the zpmt command	450
Variables for configuring deployment managers using the zpmt command	461
Variables for configuring managed (custom) nodes using the zpmt command	470
Variables for federating application servers using the zpmt command	480
Variables for configuring Network Deployment cells with application servers using the zpmt command	484
Variables for configuring administrative agents using the zpmt command	498
Variables for configuring job managers using the zpmt command	507
Variables for configuring secure proxy servers using the zpmt command.	516
Variables for configuring secure proxy administrative agents using the zpmt command	524
Using installation verification tests	533
Running installation verification tests with jobs	533
Running installation verification tests from a command line.	534
switchModules command	534
Chapter 10. Updating and uninstalling the product on z/OS	537
Adding and removing features on z/OS	537
Adding language packs on z/OS	539
Installing interim fixes and fix packs on z/OS operating systems	541
Uninstalling the product on z/OS	545
Chapter 11. Centralized installation manager (CIM)	547
Submitting Installation Manager jobs	548
Submitting jobs to install Installation Manager on remote hosts	549
Submitting jobs to update Installation Manager on remote hosts for Version 8.5	551
Submitting jobs to uninstall Installation Manager on remote hosts	553
Submitting jobs to install SSH public keys on remote hosts.	554
Installing the Version 8.5 product using the job manager and administrative console	555

Installing the Version 8.5 product using the job manager and command line	557
Managing Installation Manager using the job manager	561
Notices	569
Trademarks and service marks	571
Index	573

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

- To send comments on articles in the WebSphere Application Server Information Center
 1. Display the article in your Web browser and scroll to the end of the article.
 2. Click on the **Feedback** link at the bottom of the article, and a separate window containing an email form appears.
 3. Fill out the email form as instructed, and submit your feedback.
- To send comments on PDF books, you can email your comments to: **wasdoc@us.ibm.com**.

Your comment should pertain to specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. Be sure to include the document name and number, the WebSphere Application Server version you are using, and, if applicable, the specific page, table, or figure number on which you are commenting.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer. When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about your comments.

Using this PDF

Links

Because the content within this PDF is designed for an online information center deliverable, you might experience broken links. You can expect the following link behavior within this PDF:

- Links to Web addresses beginning with `http://` work
- Links that refer to specific page numbers within the same PDF book work
- The remaining links will *not* work. You receive an error message when you click them

Print sections directly from the information center navigation

PDF books are provided as a convenience format for easy printing, reading, and offline use. The information center is the official delivery format for IBM WebSphere Application Server documentation. If you use the PDF books primarily for convenient printing, it is now easier to print various parts of the information center as needed, quickly and directly from the information center navigation tree.

To print a section of the information center navigation:

1. Hover your cursor over an entry in the information center navigation until the **Open Quick Menu** icon is displayed beside the entry.
2. Right-click the icon to display a menu for printing or searching your selected section of the navigation tree.
3. If you select **Print this topic and subtopics** from the menu, the selected section is launched in a separate browser window as one HTML file. The HTML file includes each of the topics in the section, with a table of contents at the top.
4. Print the HTML file.

For performance reasons, the number of topics you can print at one time is limited. You are notified if your selection contains too many topics. If the current limit is too restrictive, use the feedback link to suggest a preferable limit. The feedback link is available at the end of most information center pages.

Chapter 1. What is new for installers

Installation is an easier, more consistent, and functionally rich experience across platforms, installable components, and types of installations.

Chapter 2. How do I install an application serving environment?

Follow these shortcuts to get started quickly with popular tasks.

When you visit a task in the information center, look for the **IBM Suggests** feature at the bottom of the page. Use it to find available tutorials, demonstrations, presentations, developerWorks® articles, Redbooks®, support documents, and more.

Review the software and hardware prerequisites

Plan your installation

Learn about installing the product

Prepare the base z/OS operating system

Plan for product configuration

Configure the product

Chapter 3. Task overview: Installing on z/OS

This article describes the process of installing and configuring WebSphere® Application Server for z/OS®.

Before you begin

This article introduces the context of installing and customizing IBM® WebSphere Application Server for z/OS, including the tasks you need to perform before and after installing.

To create a complete and customized WebSphere Application Server for z/OS application serving environment, you need to install the product code, prepare the z/OS operating system and subsystems, run the Profile Management Tool or **zpmf** command, follow the customized instructions and run the generated jobs, and bring up your servers.

Note: See “Building practice WebSphere Application Server for z/OS cells” on page 115 for steps you can follow to set up a practice version of WebSphere Application Server for z/OS if you want to just get the feel for it or see the basics.

About this task

Perform the following tasks to create a running version of the product on your machine.

Procedure

1. Plan your product code installation as described in Chapter 4, “Planning for product installation,” on page 23.
2. Install WebSphere Application Server for z/OS as described in Chapter 5, “Installing the product on z/OS,” on page 27.
3. Prepare your z/OS target systems to run WebSphere Application Server for z/OS as described in Chapter 7, “Preparing the base z/OS operating system,” on page 67.
4. Choose your application serving environment and decide on its initial characteristics as described in Chapter 8, “Planning for product configuration on z/OS,” on page 77.
5. Configure WebSphere Application Server for z/OS as described in Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 427.
6. To create additional application serving environments, repeat the steps in Chapter 8, “Planning for product configuration on z/OS,” on page 77 and Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 427.
7. Tune for performance.

Results

You are ready to deploy and run applications using the WebSphere Application Server for z/OS product.

WebSphere Application Server Version 8.5 product offerings for supported operating systems

WebSphere Application Server Version 8.5 includes several related offerings.

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems. The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
Application Client for IBM WebSphere Application Server com.ibm.websphere.APPLCLIENT.v85 AIX [®] , HP-UX, IBM i, Linux, Solaris, Windows	Application Client for IBM WebSphere Application Server provides resources and clients to aid development of client applications for use with WebSphere Application Server. The Application Client provides a runtime framework for client applications either to run on the Application Client machine or to be distributed with client applications that are to run on other machines.	↘ ²	↘				↘
Application Client for IBM WebSphere Application Server (ILAN) com.ibm.websphere.APPLCLIENTILAN.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	Application Client for IBM WebSphere Application Server provides resources and clients to aid development of client applications for use with WebSphere Application Server. The Application Client provides a runtime framework for client applications either to run on the Application Client machine or to be distributed with client applications that are to run on other machines. This offering is a no-cost non-supported and non-warranted version of the product.					↘	↘
DMZ Secure Proxy Server for IBM WebSphere Application Server com.ibm.websphere.NDDMZ.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	DMZ Secure Proxy Server for IBM WebSphere Application Server provides enhanced security for WebSphere Application Server environments. This offering can be used to install a proxy server in the demilitarized zone (DMZ), while reducing the security risk of installing an application server in the DMZ to host a proxy server.	↘ ³	↘				↘
DMZ Secure Proxy Server for IBM WebSphere Application Server Trial com.ibm.websphere.NDDMZTRIAL.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	DMZ Secure Proxy Server for IBM WebSphere Application Server provides enhanced security for WebSphere Application Server environments. This offering can be used to install a proxy server in the demilitarized zone (DMZ), while reducing the security risk of installing an application server in the DMZ to host a proxy server. This offering is a no-cost trial version of the product.					↘	↘
DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS com.ibm.websphere.NDDMZ.zOS.v85 z/OS	DMZ Secure Proxy Server for IBM WebSphere Application Server provides enhanced security for WebSphere Application Server for z/OS environments. This offering can be used to install a proxy server in the demilitarized zone (DMZ), while reducing the security risk of installing an application server in the DMZ to host a proxy server.	↘		↘ ⁴			↘
IBM HTTP Server for WebSphere Application Server com.ibm.websphere.IHS.v85 AIX, HP-UX, Linux, Solaris, Windows	IBM HTTP Server for WebSphere Application Server provides advanced web server capabilities with consistent management and security in a WebSphere Application Server environment. IBM HTTP Server for WebSphere Application Server is based on Apache HTTP Server.	↘ ²	↘				↘

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location							
		Product media	Presort Advantage® images ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository		
IBM HTTP Server for WebSphere Application Server (ILAN) com.ibm.websphere. IHS.LAN.v85 AIX, HP-UX, Linux, Solaris, Windows	IBM HTTP Server for WebSphere Application Server provides advanced web server capabilities with consistent management and security in a WebSphere Application Server environment. IBM HTTP Server for WebSphere Application Server is based on Apache HTTP Server. This offering is a no-cost non-supported and non-warranted version of the product.								
IBM HTTP Server for WebSphere Application Server for z/OS com.ibm.websphere. IHS.zOS.v85 z/OS	IBM HTTP Server for WebSphere Application Server for z/OS provides advanced web server capabilities with consistent management and security in a WebSphere Application Server for z/OS environment. IBM HTTP Server for WebSphere Application Server z/OS is based on Apache HTTP Server. com.ibm.websphere. IHS.zOS.v85 z/OS	↖		↖ ⁴					
IBM Web Enablement for IBM I com.ibm.websphere. WEBEMB.v85 IBM I	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. Web Enablement for IBM I offers an entitlement to WebSphere Application Server - Express®. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments of dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change.	↖			↖				
IBM WebSphere Application Server Application Server Trial com.ibm.websphere. BASE.v85 AIX, HP-UX, IBM I, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server delivers the availability and security your business depends on while optimizing cost. This base edition of WebSphere Application Server is the foundation of the IBM WebSphere software platform. WebSphere Application Server also includes the Liberty profile. ⁵	↖ ³	↖						
IBM WebSphere Application Server Trial com.ibm.websphere. BASE.ITAL.v85 AIX, HP-UX, IBM I, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server delivers the availability and security your business depends on while optimizing cost. This base edition of WebSphere Application Server is the foundation of the IBM WebSphere software platform. WebSphere Application Server also includes the Liberty profile. ⁵								
IBM WebSphere Application Server - Express com.ibm.websphere. EXPRESS.v85 AIX, HP-UX, IBM I, Linux, Solaris ⁶ , Windows	This offering is a no-cost trial version of the product. The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments of dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change. WebSphere Application Server also includes the Liberty profile. ⁵	↖ ³	↖						

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM WebSphere Application Server - Express Trial com.ibm.websphere.EXPRESS.TRIAL.v85 AIX, HP-UX, IBM i, Linux, Solaris ⁶ , Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server - Express delivers an affordable ready-to-go application foundation for smaller deployments or dynamic web applications which can be effortlessly migrated to more advanced versions of the WebSphere Application Server family as business needs change. WebSphere Application Server also includes the Liberty profile. ⁵ This offering is a no-cost trial version of the product.	↗ ³	↗			↗	↗
IBM WebSphere Application Server for Developers com.ibm.websphere.DEVELOPERS.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for Developers delivers the efficient development and innovative features of WebSphere Application Server to help developers reduce testing effort and develop with confidence using a runtime environment that is identical to the production runtime environment their applications will eventually run on. WebSphere Application Server also includes the Liberty profile. ⁵	↗ ³	↗				↗
IBM WebSphere Application Server for Developers (LAN) com.ibm.websphere.DEVELOPERS.LAN.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for Developers delivers the efficient development and innovative features of WebSphere Application Server to help developers reduce testing effort and develop with confidence using a runtime environment that is identical to the production runtime environment their applications will eventually run on. WebSphere Application Server also includes the Liberty profile. ⁵ This offering is a no-cost non-supported and non-warranted version of the product.					↗ ⁴	
IBM WebSphere Application Server for z/OS com.ibm.websphere.zOS.v85 z/OS	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server for z/OS delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications by leveraging the qualities of services of IBM System z [®] and z/OS. WebSphere Application Server also includes the Liberty profile. ⁵	↗					
IBM WebSphere Application Server Network Deployment com.ibm.websphere.ND.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server Network Deployment delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications. WebSphere Application Server also includes the Liberty profile. ⁵	↗ ³	↗				↗
IBM WebSphere Application Server Network Deployment Trial com.ibm.websphere.ND.TRIAL.v85 AIX, HP-UX, IBM i, Linux, Solaris, Windows	The IBM WebSphere Application Server family is the leading open standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation offering broad programming model choice and lower total cost of ownership through high performance and high manageability. WebSphere Application Server Network Deployment delivers near-continuous availability, with advanced performance and management capabilities for mission-critical applications. WebSphere Application Server also includes the Liberty profile. ⁵ This offering is a no-cost trial version of the product.						↗

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage® (non-z/OS systems only)	Shop Z/OS (z/OS systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM WebSphere Application Server Web 2.0 and Mobile Toolkit com.ibm.webSphere.w20tk.v11 AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	Web 2.0 and Mobile Toolkit offers targeted, incremental new features that can make your web applications running on WebSphere Application Server easier to use. With this offering, WebSphere Application Server applications that were originally developed for desktop browsers can be adapted and deployed to mobile devices such as smartphones and tablets. This offering extends Service Oriented Architecture (SOA) by connecting external web services, internal SOA services, and Java Platform, Enterprise Edition (Java EE) objects into highly-interactive web application interfaces. Web 2.0 and Mobile Toolkit provides a supported, best-in-class Ajax development toolkit for WebSphere Application Server.	✓ ³	✓	✓ ⁴		✓	✓
IBM WebSphere Application Server Web 2.0 and Mobile Toolkit (LAN) com.ibm.webSphere.w20tklan.v11 AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	Web 2.0 and Mobile Toolkit offers targeted, incremental new features that can make your web applications running on WebSphere Application Server easier to use. With this offering, WebSphere Application Server applications that were originally developed for desktop browsers can be adapted and deployed to mobile devices such as smartphones and tablets. This offering extends Service Oriented Architecture (SOA) by connecting external web services, internal SOA services, and Java Platform, Enterprise Edition (Java EE) objects into highly-interactive web application interfaces. Web 2.0 and Mobile Toolkit provides a supported, best-in-class Ajax development toolkit for WebSphere Application Server. This offering is a no-cost non-supported and non-warranted version of the product.	✓				✓	✓
IBM WebSphere Edge Components: Caching Proxy com.ibm.webSphere.EDGECP.v85 AIX, HP-UX, Linux, Solaris, Windows	WebSphere Edge Components: Caching Proxy offers efficiency and performance for WebSphere Application Server environments. This offering can satisfy multiple client requests for the same content directly from a local cache. This offering is stabilized and clients are encouraged to consider using the Proxy Server and DMZ Secure Proxy functionality provided with WebSphere Application Server Network Deployment.	✓	✓				✓
IBM WebSphere Edge Components: Load Balancer for IPv4 com.ibm.webSphere.EDGEIPV4.v85 AIX, HP-UX, Linux, Solaris, Windows	WebSphere Edge Components: Load Balancer for IPv4 offers improved performance and scalability for WebSphere Application Server in IPv4 network environments and is not intended for IPv6 network environments. This offering provides an edge-of-network system that directs network traffic flow to reduce congestion and balance incoming requests to other servers and systems. This offering is stabilized and clients are encouraged to consider using the WebSphere Edge Components: Load Balancer for IPv4 and IPv6 offering.	✓	✓				✓
IBM WebSphere Edge Components: Load Balancer for IPv4 and IPv6 com.ibm.webSphere.EDGEIPV4IPV6.v85 AIX, HP-UX, Linux, Solaris, Windows	WebSphere Edge Components: Load Balancer for IPv4 and IPv6 offers improved performance and scalability for WebSphere Application Server in IPv4 or IPv6 network environments. This offering provides an edge-of-network system that directs network traffic flow to reduce congestion and balance incoming requests to other servers and systems. This offering is a no-cost trial version of the product.	✓	✓				✓

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location					
		Product media	Passport Advantage [®] offerings ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works	Web-based repository
IBM WebSphere SDK Java Technology Edition Version 7.0 com.ibm.websphere. IBUNAV.v70	This IBM Software Development Kit (SDK) provides a full-function SDK for Java that is compliant with Java Platform, Standard Edition (Java SE) 7 application programming interfaces (APIs). With IBM WebSphere SDK Java Technology Edition Version 7.0, you can develop and deploy Java applications at the Java 7 API level and continue the "write once, run anywhere" Java paradigm at the Java API level. The SDK contains the Runtime Environment. The Runtime Environment allows users to run Java applications. The SDK also contains other tools that enable developers to create Java applications.	↘ ³	↘	↘ ⁴			↘
AIX, HP-UX, Linux, Solaris, Windows, z/OS							
Pluggable Application Client for IBM WebSphere Application Server com.ibm.websphere. PLUGCLIENT.v85	Pluggable Application Client for IBM WebSphere Application Server provides a downloadable runtime environment for Java client applications to run with the Java Runtime Environment (JRE) on the Windows platform. The Pluggable Application Client is deprecated. It is replaced by the standalone thin client, IBM Thin Client for EJB, available as part of the Application Client for IBM WebSphere Application Server offering.	↘ ²	↘				↘
Windows							
Pluggable Application Client for IBM WebSphere Application Server (ILAN) com.ibm.websphere. PLUGCLIENT_ILAN.v85	Pluggable Application Client for IBM WebSphere Application Server provides a downloadable runtime environment for Java client applications to run with the Java Runtime Environment (JRE) on the Windows platform. The Pluggable Application Client is deprecated. It is replaced by the standalone thin client, IBM Thin Client for EJB, available as part of the Application Client for IBM WebSphere Application Server offering. This offering is a no-cost non-supported and non-warranted version of the product.					↘	↘
Windows							
Web Server Plug-ins for IBM WebSphere Application Server com.ibm.websphere. PLG.v85	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server.	↘ ²	↘				↘
AIX, HP-UX, IBM i, Linux, Solaris, Windows							
Web Server Plug-ins for IBM WebSphere Application Server (ILAN) com.ibm.websphere. PLG_ILAN.v85	Web Server Plug-ins for IBM WebSphere Application Server provides an optimized connection to route requests from a web server and WebSphere Application Server. This offering is a no-cost non-supported and non-warranted version of the product.						↘
AIX, HP-UX, IBM i, Linux, Solaris, Windows							
Web Server Plug-ins for IBM WebSphere Application Server for z/OS com.ibm.websphere. PLG.zOS.v85	Web Server Plug-ins for IBM WebSphere Application Server for z/OS provides an optimized connection to route requests from a web server and WebSphere Application Server for z/OS.	↘		↘ ⁴			
z/OS							

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location				
		Product media	Presort Advantage [®] eImage ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	developer Works
WebSphere Customization Toolbox com.ibm.websphere.wct1.v85 AIX, HP-UX, Linux, Solaris, Windows ⁸	<p>The WebSphere Customization Toolbox includes tools for customizing various parts of your WebSphere Application Server environment. For example, you can use the WebSphere Customization Toolbox graphical user interface (GUI) to launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed.</p> <p>Launch the Profile Management Tool (z/OS only) on a Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems, or launch the z/OS Migration Management Tool on a Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles.</p> <p>You can use the Remote Installation Tool for IBM i to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system.</p> <p>Restriction: These tools are intended for use with the full WebSphere Application Server profile; they are not required or supported for use with the Liberty profile.</p>	<p>2</p>	<p>2</p>	<p>2</p>	<p>2</p>	<p>2</p>
WebSphere Customization Toolbox (LAN) com.ibm.websphere.wctLAN.v85 AIX, HP-UX, Linux, Solaris, Windows ⁸	<p>The WebSphere Customization Toolbox includes tools for customizing various parts of your WebSphere Application Server environment. For example, you can use the WebSphere Customization Toolbox graphical user interface (GUI) to launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed.</p> <p>Launch the Profile Management Tool (z/OS only) on a Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems, or launch the z/OS Migration Management Tool on a Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles.</p> <p>You can use the Remote Installation Tool for IBM i to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system.</p> <p>Restriction: These tools are intended for use with the full WebSphere Application Server profile; they are not required or supported for use with the Liberty profile.</p> <p>This offering is a no-cost non-supported and non-warranted version of the product.</p>					

Table 1. WebSphere Application Server Version 8.5 product offerings for supported operating systems (continued). The following table shows the WebSphere Application Server Version 8.5 product offerings for supported operating systems.

Offering, offering ID, and operating systems	Description	Location				
		Product media	Passport Advantage [®] e-images ² (non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Entitled Software Support (ESS)	Web-based repository
	<p>1 See Supported hardware and software web page for the complete up-to-date listings on what is supported. If there is a conflict between the information provided in the information center and the information on the <i>Supported hardware and software</i> pages, the information at the website takes precedence. Prerequisites information in the information center is provided as a convenience only.</p> <p>2 Located on the Supplements disk in the physical media for non-z/OS systems</p> <p>3 Located on its own disk in the physical media for non-z/OS systems</p> <p>4 Installation Manager repositories in SMP/E format, available through CBPDO or ServerPac</p> <p>5 The Liberty profile delivers a simplified and lightweight runtime environment for OSGi and web applications. Fast restart times, coupled with its small size and ease of use, make this a good option for developers building applications that do not require the full Java EE environment of traditional enterprise application-server profiles. In addition to being installable when you install the full product using Installation Manager, the Liberty profile can be downloaded and installed separately. When installed separately using downloaded files, the Liberty profile is supported on the Mac OS as well as on the platforms supported by the full WebSphere Application Server profile.</p> <p>6 IBM WebSphere Application Server - Express is not supported on Solaris x86.</p> <p>7 The Java 7 extension offering works with the following primary offerings:</p> <ul style="list-style-type: none"> • Application Client for IBM WebSphere Application Server • DMZ Secure Proxy Server for IBM WebSphere Application Server • DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS • IBM WebSphere Application Server • IBM WebSphere Application Server - Express • IBM WebSphere Application Server for Developers • IBM WebSphere Application Server for z/OS • IBM WebSphere Application Server Network Deployment <p>8 Platform-related notes:</p> <ul style="list-style-type: none"> • The Profile Management Tool (z/OS only) and z/OS Migration Management Tool that are contained in this toolbox, which create jobs to be run on z/OS systems, can be run on Intel-based Windows and Linux platforms only. • The Web Server Plugins Configuration Tool that is contained in this toolbox can be run on AIX, HP-UX, Linux, Solaris, and Windows operating systems. • The Remote Installation Tool for IBM J (the <code>!RemoteInsta11</code> command) can be run on Windows operating systems only. <p>A version of this utility that is current when the product is released is available also on the media or installation image.</p>					

Web-based service repositories for WebSphere Application Server Version 8.5 product offerings:

- 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 the table above.

- 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.

Table 2. WebSphere Application Server Version 8.5 associated products. The following table shows the products associated with WebSphere Application Server Version 8.5.

Offering	Operating systems	Description	Location			
			Product media	Passport Advantage elements (Non-z/OS systems only)	Shop ZSeries (z/OS systems only)	Web
IBM Assembly and Deploy Tools for WebSphere Administration Version 8.5	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Assembly and Deploy Tools for WebSphere Administration enable rapid assembly and deployment of applications to WebSphere Application Server environments. These tools replace the previously available IBM Rational® Application Developer Assembly and Deploy function and are restricted to assembly and deployment usage only.	✓	✓		
IBM DB2® Enterprise Server Edition Limited Use for zLinux Version 9.7	zLinux	DB2 Enterprise Server Edition is database software capable of handling demanding workloads. Designed for large and mid-sized departmental servers, Enterprise Edition should be used for applications that require flexibility and scalability.	✓	✓		
IBM DB2 Workgroup Server Edition Limited Use Version 9.7	AIX, HP-UX, Linux, Solaris, Windows	DB2 Workgroup Server Edition is a scalable, full-fledged relational database for small to medium-sized businesses.	✓	✓		
IBM Installation Manager Version 1.5.2	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Installation Manager is a single installation program that can use remote or local software repositories to install, modify, or update new 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.	✓	✓	✓ ¹	✓
IBM Packaging Utility Version 1.5.2	AIX, HP-UX, Linux, Solaris, Windows ²	IBM Packaging Utility is a program that is used to create and manage packages for repositories to be used by Installation Manager. You can generate a new repository for packages, copy multiple packages to one repository, copy multiple versions of a product to one repository, delete packages that are no longer needed, create a repository to install packages over HTTP, or copy packages from installation images or IBM repositories to a repository that resides on an internal server or a local machine for example.	✓	✓	✓ ¹	✓
IBM Rational Agent Controller Version 8.3.5	AIX, Solaris, Linux, zLinux, z/OS	IBM Rational Agent Controller is a daemon process that enables client applications to launch host processes and interact with agents that coexist within host processes.	✓	✓	✓	✓
IBM Rational Application Developer Trial Version 8.5	AIX, HP-UX, IBM i, Linux, Solaris, Windows	IBM Rational Application Developer, the enterprise software development solution for Java and Java Enterprise Edition (Java EE), helps development teams deliver solutions for WebSphere Application Server. It includes support for feature packs and integrated test servers.	✓	✓	?	
IBM Support Assistant Version 4.1.2 or Version 5	AIX, HP-UX, IBM i, Linux, Solaris, Windows, z/OS	IBM Support Assistant is a free program that simplifies support and helps users resolve questions and problems with IBM software products.	✓	✓		✓
IBM Tivoli® Access Manager for e-business Version 6.1.1	AIX, HP-UX, Linux, Solaris, Windows, z/OS	IBM Tivoli Access Manager for e-business is a user authentication, authorization, and web SSO solution for executing security policies for web and application resources.	✓	✓	✓	
IBM Tivoli Composite Application Manager for WebSphere Application Server	AIX, HP-UX, Linux, Solaris, Windows, z/OS	IBM Tivoli Composite Application Manager for WebSphere Application Server is an optional tool that can be installed after the installation of WebSphere Application Server. It monitors the performance of WebSphere Application Server applications and provides transaction response metrics and realtime status on the health of applications. You can view this data in the Tivoli Performance Viewer, which you can access from the WebSphere Application Server administrative console. This tool also provides integration with the Tivoli Application Performance Monitoring solutions.	✓	✓		✓
IBM Tivoli Directory Server Version 6.3	AIX, HP-UX, Linux, Solaris, Windows	IBM Tivoli Directory Server is an IBM implementation of the Lightweight Directory Access Protocol. IBM Tivoli Directory Server is a standards-compliant enterprise directory for corporate intranets and the Internet.	✓	✓		
IBM Tivoli Federated Identity Manager Version 6.2.2	AIX, HP-UX, Linux, Solaris, Windows	IBM Tivoli Federated Identity Manager offers secure information sharing between trusted parties with federated SSO and a security token service.	✓	✓		✓
IBM WebSphere Adapters Version 7.5.0.1 ³	Various, depending on adapter	IBM WebSphere Adapters help accelerate business integration projects with rapidly deployable, enterprise ready connections based on best practices.	✓	✓	✓	
Mozilla Firefox for AIX Version 3.5.13 (64-bit only)	AIX	Mozilla Firefox for AIX is an open source web browser. It implements technologies like the Gecko layout engine and supports Wweb standards or draft standards like HTML, XHTML, XML, CSS, DOM, and more.	✓	✓		

¹ Installation Manager repositories in SMP/E format, available through CBPDO or ServerPac

² IBM i customers can build repositories using the IBM Packaging Utility on a Windows system.

³ WebSphere Adapters Version 7.5.0.1 for WebSphere Application Server for z/OS Version 8.5 cannot be installed using the disk containing IBM WebSphere Adapters Version 7.5.0.1 on IBM WebSphere Application Server Version 8.5 Adobe Acrobat PDF and follow the z/OS installation instructions in the section on performing silent installation and uninstallation.

Directory conventions

References in product information to *app_server_root*, *profile_root*, and other directories imply specific default directory locations. This article describes the conventions in use for WebSphere Application Server.

Default product locations - z/OS

app_server_root

Refers to the top directory for a WebSphere Application Server node.

The node may be of any type—application server, deployment manager, or unmanaged for example. Each node has its own *app_server_root*. Corresponding product variables are *was.install.root* and *WAS_HOME*.

The default varies based on node type. Common defaults are *configuration_root/AppServer* and *configuration_root/DeploymentManager*.

configuration_root

Refers to the mount point for the configuration file system (formerly, the configuration HFS) in WebSphere Application Server for z/OS.

The *configuration_root* contains the various *app_server_root* directories and certain symbolic links associated with them. Each different node type under the *configuration_root* requires its own cataloged procedures under z/OS.

The default is */wasv8config/cell_name/node_name*.

plug-ins_root

Refers to the installation root directory for Web Server Plug-ins.

profile_root

Refers to the home directory for a particular instantiated WebSphere Application Server profile.

Corresponding product variables are *server.root* and *user.install.root*.

In general, this is the same as *app_server_root/profiles/profile_name*. On z/OS, this will always be *app_server_root/profiles/default* because only the profile name "default" is used in WebSphere Application Server for z/OS.

smpe_root

Refers to the root directory for product code installed with SMP/E or IBM Installation Manager.

The corresponding product variable is *smpe.install.root*.

The default is */usr/lpp/zWebSphere/V8R5*.

Hardware and software requirements on z/OS

You should be aware of the hardware and software prerequisites for installing WebSphere Application Server for z/OS.

Read the information on the WebSphere Application Server detailed system requirements website for the complete up-to-date listings of what hardware and software is required and supported.

Note: If there is a conflict between the information provided in the information center and the information on the supported hardware and software web pages, the information on the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

For more information on hardware and software requirements for installing WebSphere Application Server for z/OS, read “z/OS driving system requirements” on page 16.

For more information on hardware and software requirements for customizing and running WebSphere Application Server for z/OS application serving environments, read “z/OS target system requirements.”

z/OS driving system requirements

This article describes prerequisites for installing WebSphere Application Server for z/OS.

Hardware requirements

Read the information on the WebSphere Application Server detailed system requirements web page for the complete up-to-date listings of what hardware is required and supported.

Note: If there is a conflict between the information provided in the information center and the information on the supported hardware and software web pages, the information on the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

You should plan on four 3390-3 DASD volumes (or equivalent storage) for the product target and distribution libraries and the product HFS as well as an additional 3390-3 DASD volume (or equivalent storage) for CustomPac dialogs and work datasets (if you install using a ServerPac or SystemPac®) or for SMP/E work datasets and refile storage (if you install using a Custom-Build Product Delivery Offering).

There are significant performance advantages for those applications doing floating-point arithmetic if the machine has binary floating-point hardware.

Software requirements

Read the information on the WebSphere Application Server detailed system requirements web page for the complete up-to-date listings of what software is required and supported.

Note: If there is a conflict between the information provided in the information center and the information on the supported hardware and software web pages, the information on the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

The z/OS system used to install WebSphere Application Server for z/OS must run z/OS UNIX System Services (z/OS UNIX) with an HFS or ZFS file system configured. For details, see *z/OS UNIX System Services Planning*.

Consult the Program Directory and PSP bucket for any additional required corrective service.

z/OS target system requirements

Prerequisites for configuring and running WebSphere Application Server for z/OS application serving environments are listed below.

Hardware requirements

Read the information on the WebSphere Application Server detailed system requirements web page for the complete up-to-date listings of what hardware is required and supported.

Note: If there is a conflict between the information provided in the information center and the information on the supported hardware and software web pages, the information on the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

There are significant performance advantages for those applications doing floating point arithmetic if the machine has binary floating point hardware, such as S/390® Parallel Enterprise Server-Generation 5 and later systems.

See Basic Sizing for WebSphere Application Server on z/OS for a set of basic guidelines for determining how much real storage and DASD storage you might need.

WebSphere Application Server for z/OS is a heavy user of auxiliary storage. You might want to add additional paging volumes before configuring application serving environments.

In addition, you might want to increase your JES spool space if you use WebSphere Application Server for z/OS tracing options to the STDOUT DD dataset.

WebSphere Application Server for z/OS Version 8.5 offers full support for IBM System z[®] Application Assist Processors (zAAPs). zAAPs are designed to operate asynchronously with the general purpose processors when executing Java[™] programming under control of the IBM JVM. The IBM JVM processing cycles can be executed on the configured zAAPs with no anticipated modifications to the Java applications. The zAAPs may be purchased and installed on z9[®] – 109, z990, and z890 servers (and follow-on models only). For more details, see the IBM zAAP Redbooks at <http://www.redbooks.ibm.com/abstracts/sg246386.html?Open> .

Software requirements

Read the information on the WebSphere Application Server detailed system requirements web page for the complete up-to-date listings of what software is required and supported.

Note: If there is a conflict between the information provided in the information center and the information on the supported hardware and software web pages, the information on the website takes precedence. Prerequisites information in the information center is provided as a convenience only.

You need to enable, and configure the following z/OS elements, features, and components on each z/OS target system. Consult the WebSphere Application Server for z/OS Program Directory and PSP bucket for any additional required corrective service not listed here. In some cases, this corrective service must be installed on each target system for WebSphere Application Server to start.

- z/OS configured as a sysplex (in the case of a single z/OS system, as a monoplex)
For details, see *z/OS MVS Setting Up a Sysplex*.
- z/OS UNIX System Services (z/OS UNIX) with an HFS or ZFS file system
For details, see *z/OS UNIX System Services Planning*.
- eNetwork Communications Server (TCP/IP) or equivalent
In this documentation, we refer to eNetwork Communications Server; but you can substitute an equivalent product.
For details, see *z/OS Communications Server: IP Migration*.
- Resource recovery services (RRS)
For details, see *z/OS MVS Programming: Resource Recovery*.
- System logger
For details, see *z/OS MVS Setting up a Sysplex*.
- A security product such as z/OS Security Server (RACF[®])
In this manual, we refer to Security Server in examples; but you can substitute an equivalent security product.
For details, see *z/OS Security Server RACF Migration*.

Additional software might be required to support particular product functions.

All of the z/OS sources referenced are available at this website: <http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>

Skill requirements

In assembling your project team, you should consider the skills you need to implement WebSphere Application Server for z/OS. This article discusses the recommended skill set necessary to support the following configurations:

- Basic configurations
- Production environments

Documentation to support the z/OS skills described in this article can be found at the following website:
z/OS Internet Library

For basic configurations:

Below are the recommended skills necessary to support a basic configuration:

- z/OS UNIX System Services and the hierarchical file system (HFS) - to set up a functional HFS and UNIX environment
- eNetwork Communications Server (TCP/IP) or equivalent - to configure connectivity for WebSphere Application Server for z/OS clients and servers
- Resource recovery services (RRS) - to implement resource recovery services and to support two-phase commit transactions
- Security Server (RACF), or the security product you use - to authenticate WebSphere Application Server for z/OS clients and servers, and authorize access to resources
- Secure Sockets Layer (SSL) - to enable security if desired (recommended)
- IBM Installation Manager, SMP/E, and JCL
- System logger - to set up log streams for RRS and the WebSphere Application Server for z/OS error log
- Web server - to support HTTP clients if desired
- Workload management (WLM)
- Java and WebSphere Application Server tooling - to support application development and deployment

Depending on the needs of the applications you deploy, you might also need skills to configure the resource managers your applications require, such skills might include CICS[®], DB2, IMS[™], and MQ.

For production environments:

As you move your system toward a production environment, you need to have the following system skills available:

- Automatic restart management (ARM)
- System Automation, if you have it installed, or whichever automation you prefer to use
- Sysplex if you plan to use WebSphere Application Server for z/OS in a cell that spans systems
- Sysplex Distributor (part of eNetwork Communications Server), if you plan to create a high availability environment
- RMF[™] or other performance measurement systems

Creating implementation plans on z/OS

Create a plan for implementing your WebSphere Application Server for z/OS application serving environment

Before you begin

We assume that you have a z/OS system on which you will implement WebSphere Application Server for z/OS.

About this task

To get started, plan to build your initial WebSphere Application Server for z/OS application serving environment servers on one system, then replicate them on other systems as you expand into a cell. This procedure first guides you through initial planning and implementation of WebSphere Application Server for z/OS on a monoplex. Then, it guides you through setting up your application development and client environments. Finally, the procedure guides you through planning for optional advanced system configurations.

Perform the following steps to implement your plan, checking off each item as you complete it:

Procedure

1. Determine the skills that you need.
See “Skill requirements” on page 18 for more information.
2. Determine WebSphere Application Server for z/OS system requirements.
See “Hardware and software requirements on z/OS” on page 15 for more information.
3. Understand the security options, and prepare for securing your system.
4. Implement Workload Management in goal mode on each z/OS system if necessary.
See “z/OS workload management (WLM)” on page 99 for more information.
5. Implement Resource Recovery Services (if not already implemented) on each z/OS system.
See “Preparing Resource Recovery Services (RRS)” on page 71 for more information.
6. Plan for your performance monitoring systems.
7. Plan and define your problem diagnosis procedures.
See “Problem diagnostic plan strategy” on page 425 for more information.
8. Consider automatic restart management before you install WebSphere Application Server for z/OS.
See “Automatic restart management (ARM)” on page 421 for more information.
9. Plan your product dataset and HFS naming conventions.
10. Install the WebSphere Application Server for z/OS product.
See Chapter 5, “Installing the product on z/OS,” on page 27 for more information.
11. Prepare your z/OS target systems to run WebSphere Application Server for z/OS.
See Chapter 7, “Preparing the base z/OS operating system,” on page 67 for more information.
12. Learn about configuring application serving environments.
See Chapter 8, “Planning for product configuration on z/OS,” on page 77 for more information.
13. Set up a simple standalone application server to verify system readiness and gain experience with a basic application serving environment.
See “Building practice WebSphere Application Server for z/OS cells” on page 115 for more information.
14. Plan and define your system backup procedures.
15. Plan and define your software service procedures.
16. (Optional) Plan for testing and production systems.
17. Plan and configure the application serving environments that you want.
See Chapter 8, “Planning for product configuration on z/OS,” on page 77 and Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 427.
18. Review your administration and application security requirements and settings.
19. Develop and deploy applications.
20. Review WebSphere Application Server for z/OS requirements for application development and client environments.
21. (Optional) Implement Sysplex Distributor, and set up a high-availability environment.

22. (Optional) Expand your application serving environments as needed.
23. Tune system performance.
See “Skill requirements” on page 18 for more information.

Results

Once you have identified the elements you want to incorporate in your implementation plan, you are ready to install and configure the product.

Product file system

WebSphere Application Server for z/OS product code resides in partitioned datasets on MVS and Unix System Services file systems.

WebSphere Application Server product directory

All WebSphere Application Server for z/OS product files reside in the product directory and its subdirectories. Throughout the product and documentation, *install_root* is used to represent the fully qualified path name of the WebSphere Application Server for z/OS product directory. In the examples in the documentation, the path `/usr/lpp/zWebSphere/V8R5` normally is used as the location of the product file system.

Locate the product directory and all of its subdirectories in the same hierarchical file system (HFS) or zSeries® file system (ZFS) dataset. This dataset can be the same as the z/OS root or version dataset, which is not recommended, or a separate dataset that is used just for WebSphere Application Server for z/OS. The installation jobs and program directory assume that such a separate dataset is allocated. This dataset is referred to as *was_hlq.SBBOHFS*, where *was_hlq* represents the product dataset name high-level qualifiers. This directory gets created during the installation process.

Refer to the Program Directory on the WebSphere Application Server library web page for more details.

DMZ Secure Proxy Server product directory

The DMZ Secure Proxy Server for WebSphere Application Server files reside in the DMZ Secure Proxy Server product directory and its subdirectories. In the examples in this documentation, the path `/usr/lpp/zWebSphere_SPS/V8R5` normally is used as the location of the DMZ Secure Proxy Server product file system.

Web Server Plug-ins product directory

The Web Server Plug-ins for WebSphere Application Server files reside in the Web Server Plug-ins product directory and its subdirectories. In the examples in this documentation, the path `/usr/lpp/zWebSphere_Plugins/V8R5` normally is used as the location of the Web Server Plug-ins product file system.

On z/OS, plug-ins are provided for the IBM HTTP Server (IHS/390) that is provided with the z/OS operating system and for the IBM HTTP Server (based on Apache) that is provided with either WebSphere Application Server for z/OS or with the IBM Ported Tools for z/OS.

Product directory and configuration directory

Each WebSphere Application Server for z/OS application serving environment (standalone application server node or Network Deployment cell) has configuration files in one or more WebSphere configuration directories. These configuration directories are created through the configuration process and contain symbolic links to files in the WebSphere Application Server product directory.

DMZ secure proxy servers and secure proxy administrative agents have symbolic links to files in the DMZ Secure Proxy Server product directory.

Using indirection to isolate product directories

Instead of pointing directly to these product directories, application serving environments can point to an intermediate symbolic link, which in turn points to a particular product directory. This level of indirection allows you to switch to a new server level of WebSphere Application Server for z/OS or the DMZ Secure Proxy server by stopping the servers that use that intermediate symbolic link, changing the link to point to the new product directory, and restarting the affected servers.

The customization process allows for automatic creation of these intermediate symbolic links.

Chapter 4. Planning for product installation

WebSphere Application Server Version 8.5 is installed using IBM Installation Manager. This article outlines the issues that you should consider in planning your product installation.

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, console mode, or response files.

For more information on using Installation Manager, read the IBM Installation Manager Version 1.5 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.

To manage multiple copies of a software product—a test copy and a production copy for example—you install the product several times and into separate package groups, each with a distinct installation location. The different copies of the product can be maintained or upgraded separately.

Installation Manager modes

IBM Installation Manager can be installed in one of the following three modes:

- In admin mode, the Installation Manager is installed from a superuser ID and can be invoked by any superuser.
A file pointing to the Installation Manager is created in `/etc/.ibm/registry`; therefore, there can only be one admin-mode Installation Manager on a z/OS system.
- In nonAdmin mode (also called user mode), the Installation Manager can be invoked only by the user that installed it.
A file pointing to the Installation Manager is created in `$HOME/etc/ibm/registry`; therefore, there can only be one user-mode Installation Manager for a user.
- In group mode, the Installation Manager can be invoked by any user ID that is connected to the default group of the user that installed it.
A file pointing to the Installation Manager is created in `appdata_location/etc/.ibm/registry`. So there is no limit to the number of group-mode Installation Managers per system or user as long as each has its own appdata location.

How many Installation Managers do I 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.

Getting the Installation Manager installation kit

IBM Installation Manager comes in the form of an installation kit, which contains a set of Installation Manager binaries and a repository for the Installation Manager product. On z/OS, the Installation Manager installation kit normally resides at `/usr/lpp/InstallationManager/V1R5`. A copy of the Installation Manager installation kit is provided in SMP/E format with the WebSphere Application Server Version 8.5 product.

The installation kit is only used for setup and maintenance of the Installation Manager.

Creating an Installation Manager

When the installation kit is available on your z/OS 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.

The initial product repository for WebSphere Application Server Version 8.5 for z/OS is installed on your system with SMP/E. This SMP/E-installed repository will be updated over time to include regular product service in the form of fix packs.

You can also have Installation Manager download product fix packs and interim fixes from an IBM service website. Note that interim fixes will be available only through the service website or from the IBM Support Center.

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, console mode, 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.

Each copy of a product must be installed at a separate installation location (file system path). Certain products might be intended to be installed together into a common location.

Choosing installation locations is a critical part of product planning. These installation locations will normally be distinct from the locations at which the products are mounted when actually in use.

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 Version 8.5 products by issuing the `versionInfo.sh` command from the product file system.

After products are installed, you can unmount them from the locations at which they are known to Installation Manager and remount them at other production locations or you can copy them to other computer systems. If you copy the Installation Manager binaries and runtime data along with the product file system, you can apply maintenance to the installed products on any computer system that has access to the product and service repositories.

You can use Installation Manager commands, console mode, 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.

Chapter 5. Installing the product on z/OS

You install the product using IBM Installation Manager. Installation Manager installs products from one or more product repositories.

About this task

To install the WebSphere Application Server for z/OS Version 8.5 product, 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, perform one of the following procedures:
 - Install the Installation Manager installation kit (FMID HGIN140) 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: You can download an unzip utility from z/OS Unix System Services ported tools.

- Access to a copy of the product repository
 - Perform one of the following procedures:
 - Install the WebSphere Application Server Version 8.5 repository (FMID HBBO850) using SMP/E.
 - Copy the compressed product repositories from the product media to your z/OS system, and uncompress them.

Procedure

1. Create an Installation Manager.
 - Perform the following procedures:
 - “Obtaining an Installation Manager installation kit for installing the product on z/OS”
 - “Creating an Installation Manager for installing the product on z/OS” on page 28
2. Obtain the product repositories.
 - Perform the following procedure: “Obtaining product repositories for installing the product on z/OS” on page 31.
3. Install WebSphere Application Server for z/OS Version 8.5.
 - Perform the following procedure: “Installing WebSphere Application Server for z/OS” on page 33.

What to do next

You can use Installation Manager to install the DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS, 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.

Go to the information center for information on configuring WebSphere Application Server for z/OS.

Obtaining an Installation Manager installation kit for installing the product on z/OS

The installation kit for the IBM Installation Manager is provided with the WebSphere Application Server for z/OS Version 8.5 product 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 for z/OS Version 8.5 product 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 1.5.2, the minimum Installation Manager level for WebSphere Application Server Version 8.5.
Mount the installation kit file system at a location of your choice.
 - If you ordered the WebSphere Application Server for z/OS Version 8.5 product 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 product following the instructions in the Installation Manager program directory. PTFs must be installed to bring the installation kit up to Installation Manager 1.5.2, the minimum Installation Manager level for WebSphere Application Server Version 8.5.
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:
See the IBM Installation Manager Version 1.5 Information Center for download and extraction instructions. Make sure to download an installation kit that is at Installation Manager Version 1.5.2 or above.
Mount the resulting installation kit file system at a location of your choice.
The installation kit file system can be mounted read-only after it is installed with SMP/E or downloaded and extracted. It is not modified during Installation Manager processing.

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 the product on z/OS.”

Creating an Installation Manager for installing the product on z/OS

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 Version 8.5, your Installation Manager must be at Version 1.5.2 or above.

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 3. 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.

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 below 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.

The installation kit must be at Version 1.5.2 or above.

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 above 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 above, 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 product repositories for installing the product on z/OS

WebSphere Application Server Version 8.5 products 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 for z/OS Version 8.5 product can be obtained by one of the following methods:

- Installing with SMP/E using a ServerPac, SystemPac, or Customer-Build Product Delivery Offering (CBPDO)
This results in a repository file system containing the initial repositories for WebSphere Application Server for z/OS, DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS, 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.
- Copying the initial (compressed) product repositories from the product physical media or ShopzSeries to your z/OS system, and uncompressing them

New service levels can be installed from the web-based service repositories or downloaded as service repositories that contain additional product code. Each service repository contains all the necessary materials to upgrade any previous service level of WebSphere Application Server Version 8.5 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 for z/OS Version 8.5.

Procedure

- To install initial repositories using SMP/E, perform the following procedure.
 1. Order an IBM ServerPac, SystemPac, or CBPDO for the WebSphere Application Server for z/OS Version 8.5 product.

It will contain the following FMIDs:

HBBO850

Product repository for WebSphere Application Server for z/OS, DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS, IBM HTTP Server for z/OS, and Web Server Plug-ins for WebSphere Application Server for z/OS

HBBJ700

Product repository for IBM WebSphere SDK Java Technology Edition Version 7.0

This FMID is only needed if you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 with WebSphere Application Server Version 8.5.

2. 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/HBB0850
```

If you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 with WebSphere Application Server Version 8.5, mount the optional repository at a location of your choice as well. In the examples in this documentation, these repositories are mounted at:

```
/usr/lpp/InstallationManagerRepository/HBBJ700
```

- To install initial repositories without SMP/E, perform the following procedure.
 1. Copy the following files from the product media to your z/OS system. If you use FTP, be sure to transfer the files in binary format.

was.repo.8500.zOS.zip

Initial repository for WebSphere Application Server for z/OS and DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS

was.repo.8500.plugins.zip

Initial repository for Web Server Plug-ins for WebSphere Application Server for z/OS

was.repo.8500.ihs.zip

Initial repository for IBM HTTP Server for z/OS

Uncompress each file into an empty directory. You can download an unzip utility from z/OS Unix System Services ported tools.

2. If you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 with WebSphere Application Server Version 8.5, 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.8500.java7.zip

Initial repository for IBM WebSphere SDK Java Technology Edition Version 7.0

Uncompress the file into an empty directory. You can download an unzip 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 containing materials for WebSphere Application Server for z/OS, DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS, IBM HTTP Server for z/OS, and Web Server Plug-ins for WebSphere Application Server for z/OS as well as a second (optional) file system containing the IBM WebSphere SDK Java Technology Edition Version 7.0 repository. Each repository file system contains the initial product level. If PTFs were installed, each repository file system will also contain a single product service level.

If you installed the initial repositories without SMP/E, you now have separate directories containing the initial product repositories for WebSphere Application Server for z/OS, DMZ Secure Proxy Server for IBM WebSphere Application Server 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 (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 for z/OS, including DMZ Secure Proxy Server for IBM WebSphere Application Server 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.

What to do next

When you use IBM Installation Manager to install WebSphere Application Server Version 8.5 products, specify the path to the appropriate repository in the `-repositories` parameter of the `imc1` command.

Installing WebSphere Application Server for z/OS

The product code for WebSphere Application Server for z/OS Version 8.5 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 for z/OS Version 8.5. The repository can be mounted read-only.

Procedure

1. Choose an installation location for this copy of WebSphere Application Server for z/OS Version 8.5. 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 35,000 tracks (3390) or 1800 megabytes. 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.z0S.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 732Ukelele  
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.z0S.v85/repository.xml
```

Make sure that the keyring file is readable by the Installation Manager user ID.

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 for z/OS Version 8.5 offering, `com.ibm.websphere.zOS.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 for z/OS product.

```
imcl install com.ibm.websphere.zOS.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 product.

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 the WebSphere Application Server base product. The keyword name for each feature is provided in parentheses.

- WebSphere Application Server full profile (`core.feature`)

Installing this application-server feature gives you the traditional standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation, offering broad programming model choice and low total cost of ownership through high performance and high manageability.

- EJBDeploy tool for pre-EJB 3.0 modules (`ejbdeploy`)

This optional feature contains the EJBDeploy tool for pre-EJB 3.0 modules.

Before you deploy applications on the server, you must run the EJBDeploy tool on applications that contain EJB modules that are based on specifications prior to EJB 3.0. Running the EJBDeploy tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature called JITDeploy, which automatically generates code when the application starts.

- Standalone thin clients and resource adapters (`thinclient`)

This optional feature contains the IBM standalone thin clients and resource adapters. IBM thin clients provide a set of clients for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.

- Embeddable EJB container (`embeddablecontainer`)

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 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.

- Sample applications (`samples`)

This optional feature contains the PlantsByWebSphere sample application. The samples feature is recommended for installation in learning and demonstration environments, such as development environments; however, it is not recommended for installation in production application server environments.

- WebSphere Application Server Liberty profile (`liberty`)

Installing this application-server feature gives you a lightweight profile of the application server along with a simplified configuration approach for the development environment. Its fast restart times, small size, and ease of use make it a good option for building web applications that do not require the full JEE environment of traditional enterprise application server profiles. The Liberty profile also can be used in production; and because it is a dynamic configuration, the application server provisions only the features required by the running applications.

Note: The Liberty profile is installed into the `wlp` subdirectory of the WebSphere Application Server installation directory.

Notes:

- When you install a new copy of the WebSphere Application Server for z/OS and do not specify the features to be installed, the following features are installed by default:
 - `core.feature`
 - `ejbdeploy`
 - `thinclient`
 - `embeddablecontainer`
- If any features are listed, the normal list of default features is ignored and only the listed features are installed.
- You must install `core.feature` (full WebSphere Application Server profile), `liberty` (Liberty profile), or both.
- You cannot use the Installation Manager modify, update, or rollback functions to modify this installation later and add or remove `core.feature` (full WebSphere Application Server profile) or `liberty` (Liberty profile). You can use these functions to add or remove the `ejbdeploy`, `thinclient`, `embeddablecontainer`, or `samples` subfeature of `core.feature` later.

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 WebSphere Application Server nodes and servers.

What to do next

You can now install other WebSphere Application Server components or configure an application-serving environment with the WebSphere Customization Toolbox or the `zpmc.sh` command.

Installing IBM WebSphere SDK Java Technology Edition Version 7.0

The product code for IBM WebSphere SDK Java Technology Edition Version 7.0 is installed 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 for z/OS Version 8.5 .
3. Obtain the product repository for IBM WebSphere SDK Java Technology Edition Version 7.0. The repository can be mounted read-only.

Procedure

1. Choose the installed copy of WebSphere Application Server for z/OS Version 8.5 onto which you will install IBM WebSphere SDK Java Technology Edition Version 7.0.
2. Mount the product file system for this copy of WebSphere Application Server 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 20,000 tracks (3390) or 1,100 megabytes of free disk space to install IBM WebSphere SDK Java Technology Edition Version 7.0.

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.SIWOHFS -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.

```
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.IBMJAVA.v70/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:

```
/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.IBMJAVA.v70/repository.xml
```

Make sure that the keyring file is readable by the Installation Manager user ID.

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 offering, `com.ibm.websphere.IBMJAVA.v70`.

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. Run the Installation Manager command-line tool to install IBM WebSphere SDK Java Technology Edition Version 7.0.

```
imcl install com.ibm.websphere.IBMJAVA.v70
-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 WebSphere Application Server nodes and servers.

What to do next

You can now install other WebSphere Application Server components or configure an application-serving environment.

Installing DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS

The product code for DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS Version 8.5 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 for z/OS Version 8.5. The repository can be mounted read-only.

Procedure

1. Choose an installation location for this copy of DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS Version 8.5.

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. Do not install DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS into a location used by any other product.

2. Mount an empty file system read/write at this location.

It will require a minimum of 21,000 tracks (3390) or 900 megabytes. 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_SPS/V8R5
```

```
chmod 775 /usr/lpp/zWebSphere_SPS/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.SDYZHFS -type ZFS  
-megabytes 900 100 -volume PRV005  
-mountpoint /usr/lpp/zWebSphere_SPS/V8R5  
-owner IMADMIN -group IMGROUP
```

If you installed the initial product repository with SMP/E, you can use sample job BBO2CFS 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.NDDMZ.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 732Ukelele  
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.NDDMZ.zOS.v85/repository.xml
```

Make sure that the keyring file is readable by the Installation Manager user ID.

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 DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS Version 8.5 offering, `com.ibm.websphere.NDDMZ.zOS.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 DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS product.

```
imcl install com.ibm.websphere.NDDMZ.zOS.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 product.

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 add a list of features that are separated by commas—for example, the feature ID `thinClient` indicates the standalone thin clients and resource adapters. If any features are listed, the normal list of default features is ignored and only the listed features are installed.

If you installed the initial product repository with SMP/E, you can use sample job BBO2INST 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 file system and remount it read-only for use by DMZ Secure Proxy Server for IBM WebSphere Application Server nodes and servers.

What to do next

You can now install other WebSphere Application Server components or configure your application-serving environment for DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS.

Installing Web Server Plug-ins for IBM WebSphere Application Server for z/OS

The product code for Web Server Plug-ins for IBM WebSphere Application Server for z/OS Version 8.5 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 for z/OS Version 8.5. The repository can be mounted read-only.

Procedure

1. Choose an installation location for this copy of Web Server Plug-ins for IBM WebSphere Application Server for z/OS Version 8.5.

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. Do not install the Web Server Plug-ins for IBM WebSphere Application Server for z/OS into a location used by any other product.

2. Mount an empty file system read/write at this location.

It will require a minimum of 1,000 tracks (3390) or 50 megabytes. 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_Plugins/V8R5
```

```
chmod 775 /usr/lpp/zWebSphere_Plugins/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.SIWOHFS -type ZFS  
-megabytes 50 10 -volume PRV005  
-mountpoint /usr/lpp/zWebSphere_Plugins/V8R5  
-owner IMADMIN -group IMGROUP
```

If you installed the initial product repository with SMP/E, you can use sample job BBO3CFS 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.PLG.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 732Ukelele  
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.PLG.zOS.v85/repository.xml
```

Make sure that the keyring file is readable by the Installation Manager user ID.

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 Web Server Plug-ins for IBM WebSphere Application Server for z/OS Version 8.5 offering, `com.ibm.websphere.PLG.zOS.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 Web Server Plug-ins for IBM WebSphere Application Server for z/OS product.

```
imcl install com.ibm.websphere.PLG.zOS.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 product.

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`.

If you installed the initial product repository with SMP/E, you can use sample job BBO3INST 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 file system and remount it read-only for use by WebSphere Application Server nodes and servers.

What to do next

You can now install other WebSphere Application Server components or configure an application-serving environment for Web Server Plug-ins for IBM WebSphere Application Server for z/OS.

Chapter 6. Installing and using the WebSphere Customization Toolbox

The WebSphere Customization Toolbox include tools for managing, configuring, and migrating various parts of your WebSphere Application Server environment.

About this task

The WebSphere Customization Toolbox for WebSphere Application Server Version 8.5 includes tools for customizing various parts of your WebSphere Application Server environment.

- You can launch the Web Server Plug-ins Configuration Tool to configure your web server plug-ins for any operating system on which the WebSphere Customization Toolbox can be installed.
You can also use the WCT command-line utility to launch the command-line version of the Plug-ins Configuration Tool, the **pct** tool.
- You can launch the Profile Management Tool (z/OS only) on an Intel-based Windows or Linux operating system to generate jobs and instructions for creating profiles for WebSphere Application Server on z/OS systems.
- You can launch the z/OS Migration Management Tool on an Intel-based Windows or Linux operating system to generate definitions for migrating WebSphere Application Server for z/OS profiles.

Procedure

Perform one of the following procedures:

- Install and use the WebSphere Customization Toolbox GUI to invoke the following tools.
 - Profile Management Tool (z/OS only)
The Profile Management Tool (z/OS only) allows you to build and process definitions for creating WebSphere Application Server profiles.
Processing the definitions results in the generation of customization jobs that you then run on the z/OS system. You can upload directly to the z/OS system as you process a definition, or you can save it locally and upload it to the z/OS system later.
 - z/OS Migration Management Tool
The z/OS Migration Management Tool allows you to build and process definitions for migrating WebSphere Application Server profiles.
Processing the definitions results in the generation of customization jobs that you then run on the z/OS system. You can upload directly to the z/OS system as you process a definition, or you can save it locally and upload it to the z/OS system later.
 - Web Server Plug-ins Configuration Tool
The Web Server Plug-ins Configuration Tool allows you to configure your web server plug-ins on distributed and Windows operating systems.
- Use the WCT command to invoke the pct tool to configure your web server plug-ins on distributed and Windows operating systems.

What to do next

Restriction:

You cannot use some combinations of the GUI customization tools for IBM WebSphere Application Server Version 8.5 concurrently.

- You cannot have the following two tools or two instances of either tool open at the same time:

- Profile Management Tool for distributed operating systems
- Configuration Migration Tool for distributed operating systems
- You cannot have two of the following tools within the WebSphere Customization Toolbox or two instances of any one tool open at the same time:
 - Web Server Plug-ins Configuration Tool
 - Profile Management Tool (z/OS only), which runs on Intel-based Windows or Linux operating systems
 - z/OS Migration Management Tool, which runs on Intel-based Windows or Linux operating systems

You can use one tool from one of these two sets and one tool from the other set at the same time.

Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox

IBM Installation Manager is a common installer for many IBM software products that you use to install, update, roll back, and uninstall the WebSphere Customization Toolbox.

Before you begin

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 or later.

About this task

The WebSphere Customization Toolbox contains the following optional tools:

- Web Server Plug-ins Configuration Tool

The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.

Note: This tool can be installed and run on AIX, HP-UX, Linux, Solaris systems.

- Profile Management Tool (z/OS only)

The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- z/OS Migration Management Tool

The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

The `iRemoteInstall` command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The `iRemoteInstall` command is installed into the following directory:

`wct_root/Remote_Installation_Tool_for_IBM_i`

Restriction: This tool can be installed and run on Windows operating systems only.

Restriction: These tools are intended for use with the full WebSphere Application Server profile; they are not required or supported for use with the Liberty profile.

Perform one of these procedures to install, update, roll back, or uninstall the WebSphere Customization Toolbox using Installation Manager.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on distributed operating systems using the command line
- Uninstalling fix packs from distributed operating systems using the command line

Procedure

- “Installing the WebSphere Customization Toolbox using the GUI”
- “Installing the WebSphere Customization Toolbox using response files” on page 49
- “Installing the WebSphere Customization Toolbox using the command line” on page 55
- “Installing and removing tools in the WebSphere Customization Toolbox” on page 59
- “Installing fix packs on the WebSphere Customization Toolbox using the GUI” on page 61
- “Uninstalling fix packs from the WebSphere Customization Toolbox using the GUI” on page 62
- “Uninstalling the WebSphere Customization Toolbox using the GUI” on page 62
- “Uninstalling the WebSphere Customization Toolbox using response files” on page 63
- “Uninstalling the WebSphere Customization Toolbox using the command line” on page 65

What to do next

The **versionInfo** and **historyInfo** commands return version and history information for the WebSphere Customization Toolbox based on all of the installation, uninstallation, update, and rollback activities performed on the system.

Installing the WebSphere Customization Toolbox using the GUI

You can use the Installation Manager GUI to install the WebSphere Customization Toolbox.

Before you begin

Install Installation Manager:

1. Perform one of the following procedures:

- If you want to use the Installation Manager that is included with this product, perform the following actions:

a. 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 product media.

1) Install Installation Manager on your system.

You can install Installation Manager using the product 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.

2) Use Installation Manager to install the product from the product repositories on the media.

– **Download the files from the product website, and use local installation**

You can download the necessary product repositories from the product website.

- 1) Download the files from the product website.
- 2) Install Installation Manager on your system.

You can install Installation Manager using the product 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.

- 3) Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

You can install the product from the web-based repositories.

- 1) Install Installation Manager on your system.

You can install Installation Manager using the product 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.

- 2) Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.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 `imc1` 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.

- 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, and Solaris:** `./install`

Non-administrative installation:

- **Windows:** `userinst.exe`
- **AIX, HP-UX, Linux, and Solaris:** `./userinst`

Group-mode installation (AIX, HP-UX, Linux, and Solaris only):

`./groupinst -dataLocation application_data_location`

Notes on group mode:

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- 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 Version 1.5 Information Center before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Version 1.5 Information Center.

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.
- If you already have Installation Manager Version 1.5.2 or later 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 product media. Use Installation Manager to install the product from the product repositories on the media.

– **Download the files from the product website, and use local installation**

You can download the necessary product repositories from the product website.

- a. Download the product repositories from the product website.
- b. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

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.WCT.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.

2. Add the product repository to your Installation Manager preferences.
 - a. Start Installation Manager.
 - b. In the top menu, 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\product_name\local-repositories`
 - **AIX, HP-UX, Linux, Solaris:** `/var/repositories/product_name/local-repositories`
 or
 - 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.

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v85>

Procedure

1. Start Installation Manager.

Tip: On AIX, HP-UX, Linux, and Solaris systems, 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 Version 1.5 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 following actions.

- a. Select **WebSphere Customization Toolbox** and the appropriate version.

If you already have the WebSphere Customization Toolbox installed on your system, a message displays indicating that the WebSphere Customization Toolbox is already installed. To create another installation of the WebSphere Customization Toolbox 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 Version 1.5 Information Center for information about automatic updates.

4. Accept the terms in the license agreements, and click **Next**.

5. Specify the installation root directory for the tool 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.

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.
The WebSphere Customization Toolbox cannot install properly if the target directory includes a semicolon.
- The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

6. Click **Next**.

7. Select the tools that you want to install.

Choose from the following optional tools:

- Web Server Plug-ins Configuration Tool

The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.

- Profile Management Tool (z/OS only)

The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- z/OS Migration Management Tool

The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

The **iRemoteInstall** command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The **iRemoteInstall** command is installed into the following directory:

`wct_root/Remote_Installation_Tool_for_IBM_i`

Restriction: This tool can be installed and run on Windows operating systems only.

Note: If you install the z/OS Migration Management Tool, you must also install the Profile Management Tool (z/OS only). This selection is done automatically.

8. Click **Next**.

9. 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.

10. Optional: Select **None** to deselect **WebSphere Customization Toolbox** if you do not want to open the WebSphere Customization Toolbox when this installation is finished.

11. Click **Finish**.

12. Click **File > Exit** to close Installation Manager.

Installing the WebSphere Customization Toolbox using response files

You can install the WebSphere Customization Toolbox using Installation Manager response files.

Before you begin

Install Installation Manager on each of the systems onto which you want to install the product.

- If you want to use the Installation Manager that is included 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 product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product 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 product website, and use local installation**

You can download the necessary product repositories from the product website.

- a. Download the files from the product website.

- b. Install Installation Manager on your system.

You can install Installation Manager using the product 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**

You can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product 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.WCT.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.

2. Change to the location containing the Installation Manager installation files, and run one of the following commands:

Administrative installation:

- **Windows:** `installc.exe -acceptLicense -log log_file_path_and_name`
- **AIX, HP-UX, Linux, and Solaris:** `./installc -acceptLicense -log log_file_path_and_name`

Non-administrative installation:

- **Windows:** `userinstc.exe -acceptLicense -log log_file_path_and_name`
- **AIX, HP-UX, Linux, and Solaris:** `./userinstc -acceptLicense -log log_file_path_and_name`

Group-mode installation (AIX, HP-UX, Linux, and Solaris only):

`./groupinstc -acceptLicense -dataLocation application_data_location -log log_file_path_and_name -installationDirectory Installation_Manager_home`

Notes on group mode:

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
 - 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 Version 1.5 Information Center before installing in group mode.
 - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Version 1.5 Information Center.
- If you already have Installation Manager Version 1.5.2 or later 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 product media. Use Installation Manager to install the product from the product repositories on the media.

- **Download the files from the product website, and use local installation**

You can download the necessary product repositories from the product website.

1. Download the product repositories from the product website.
2. Use Installation Manager to install the product from the downloaded repositories.

- **Access the live repositories, and use web-based installation**

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.WCT.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.

About this task

Using Installation Manager, you can work with response files to install the WebSphere Customization Toolbox 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 the WebSphere Customization Toolbox:** On one of your systems, perform the following actions to record a response file that will install the WebSphere Customization Toolbox.
 - 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, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/install_response_file.xml
```

- **AIX, HP-UX, Linux, or 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 Version 1.5 Information Center.

- c. Add the appropriate repositories to your Installation Manager preferences.

- 1) In the top menu, 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.WCT.v85>

- Local repositories:

- **Windows:** `C:\repositories\wct\local-repositories`

- **AIX, HP-UX, Linux, Solaris:** `/var/repositories/wct/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 following actions.

- 1) Select **WebSphere Customization Toolbox** and the appropriate version.

If you already have the WebSphere Customization Toolbox installed on your system, a message displays indicating that the WebSphere Customization Toolbox is already installed. To create another installation of the WebSphere Customization Toolbox in another location, 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**.

f. Accept the terms in the license agreements, and click **Next**.

g. Specify the installation root directory for the WebSphere Customization Toolbox 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.

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.
The WebSphere Customization Toolbox cannot install properly if the target directory includes a semicolon.
- The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

h. Click **Next**.

i. Select the features (tools) that you want to install.

Choose from the following optional tools:

- Web Server Plug-ins Configuration Tool

The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.

- Profile Management Tool (z/OS only)

The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- z/OS Migration Management Tool

The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

The **iRemoteInstall** command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The **iRemoteInstall** command is installed into the following directory:

`wct_root/Remote_Installation_Tool_for_IBM_i`

Restriction: This tool can be installed and run on Windows operating systems only.

Note: If you install the z/OS Migration Management Tool, you must also install the Profile Management Tool (z/OS only). This selection is done automatically.

- j. Click **Next**.
- k. 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.
- l. Optional: Select **None** to deselect **WebSphere Customization Toolbox** if you do not want to open the WebSphere Customization Toolbox when this installation is finished.

This option is unavailable if you used the `-skipInstall` parameter.

- m. Click **Finish**.
- n. Click **File > Exit** to close Installation Manager.
- o. Optional: If you are using an authenticated remote repository, create a keyring file for installation.
 - 1) From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
 - 2) Start Installation Manager from the command line using the `-record` option.

For example:

- **Windows administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-keyring C:\IM\im.keyring  
-record C:\temp\keyring_response_file.xml
```

- **AIX, HP-UX, Linux, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-keyring /var/IM/im.keyring  
-record /var/temp/keyring_response_file.xml
```

- **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-keyring user_home/var/IM/im.keyring  
-record user_home/var/temp/keyring_response_file.xml
```

- 3) When a window opens that requests your credentials for the authenticated remote repository, enter the correct credentials and **save** them.
- 4) Click **File > Exit** to close Installation Manager.

For more information, read the IBM Installation Manager Version 1.5 Information Center.

2. Use the response files to install the WebSphere Customization Toolbox:

- a. Optional: **Use the response file to install the keyring:** Go to a command line on each of the systems on which you want to install the WebSphere Customization Toolbox, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the keyring.

For example:

- **Windows administrator or non-administrator:**

```
imcl.exe -acceptLicense  
input C:\temp\keyring_response_file.xml  
-log C:\temp\keyring_log.xml
```

- **AIX, HP-UX, Linux, or Solaris administrator:**

```
./imcl -acceptLicense  
input /var/temp/keyring_response_file.xml  
-log /var/temp/keyring_log.xml
```

- **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./imcl -acceptLicense  
input user_home/var/temp/keyring_response_file.xml  
-log user_home/var/temp/keyring_log.xml
```


- b. **Use the response file to install the WebSphere Customization Toolbox:** Go to a command line on each of the systems on which you want to install the WebSphere Customization Toolbox, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the WebSphere Customization Toolbox.

For example:

- **Windows administrator or non-administrator:**

```
imcl.exe -acceptLicense
input C:\temp\install_response_file.xml
-log C:\temp\install_log.xml
-keyring C:\IM\im.keyring
```

- **AIX, HP-UX, Linux, or Solaris administrator:**

```
./imcl -acceptLicense
input /var/temp/install_response_file.xml
-log /var/temp/install_log.xml
-keyring /var/IM/im.keyring
```

- **AIX, HP-UX, Linux, or Solaris non-administrator:**

```
./imcl -acceptLicense
input user_home/var/temp/install_response_file.xml
-log user_home/var/temp/install_log.xml
-keyring user_home/var/IM/im.keyring
```

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 Version 1.5 Information Center for more information.

Example

The following is an example of a response file for installing all of the WebSphere Customization Toolbox.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v85" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.WCT.v85'
profile='WebSphere Customization Toolbox V8.5'
features='core.feature,pct,zpmt,zmmt' installFixes='none' />
</install>
<profile id='WebSphere Customization Toolbox V8.5'
installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox' />
<data key='user.import.profile' value='false' />
<data key='user.select.64bit.image.com.ibm.websphere.WCT.v85' value='false' />
<data key='cic.selector.nl' value='en' />
</profile>
</agent-input>
```

Tip: To select the features (tools) that you want to install, add each desired feature in the offering as an entry in a comma-separated list. To install all of the optional features, for example, specify something like this:

```
<offering profile='WebSphere Customization Toolbox V8.5'
features='core.feature,zpmt,zmmt,pct,installtools' id='com.ibm.websphere.WCT.v85' />
```

where `zpmt` indicates the Profile Management Tool (z/OS only), `zmmt` indicates the z/OS Migration Management Tool, `pct` indicates the Web Server Plug-ins Configuration Tool, and `installtools` indicates the Remote Installation Tool for IBM i.

Installing the WebSphere Customization Toolbox using the command line

You can install the WebSphere Customization Toolbox using the Installation Manager command line.

Before you begin

Important: Before installing the product, 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 below.

Install Installation Manager on each of the systems onto which you want to install the product.

- If you want to use the Installation Manager that is included 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 product media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product 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 product website, and use local installation**

You can download the necessary product repositories from the product website.

- a. Download the files from the product website.

- b. Install Installation Manager on your system.

You can install Installation Manager using the product 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**

You can install the product from the web-based repositories.

- a. Install Installation Manager on your system.

You can install Installation Manager using the product 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.WCT.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.

2. Change to the location containing the Installation Manager installation files, and run one of the following commands:

Administrative installation:

- **Windows:** `installc.exe -acceptLicense -log log_file_path_and_name`
- **AIX, HP-UX, Linux, and Solaris:** `./installc -acceptLicense -log log_file_path_and_name`

Non-administrative installation:

- **Windows:** `userinstc.exe -acceptLicense -log log_file_path_and_name`

- **AIX, HP-UX, Linux, and Solaris:** `./userinstc -acceptLicense -log log_file_path_and_name`

Group-mode installation (AIX, HP-UX, Linux, and Solaris only):

`./groupinstc -acceptLicense -dataLocation application_data_location -log log_file_path_and_name -installationDirectory Installation_Manager_home`

Notes on group mode:

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
 - 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 Version 1.5 Information Center before installing in group mode.
 - For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Version 1.5 Information Center.
- If you already have Installation Manager Version 1.5.2 or later 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 product media. Use Installation Manager to install the product from the product repositories on the media.

- **Download the files from the product website, and use local installation**

You can download the necessary product repositories from the product website.

1. Download the product repositories from the product website.
2. Use Installation Manager to install the product from the downloaded repositories.

- **Access the live repositories, and use web-based installation**

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.WCT.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.

Procedure

1. Optional: If the repository requires a username and password, create a keyring file to access this repository.

For more information on creating a keyring file for Installation Manager, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring 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.

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 product repository is available.

Windows:

```
imcl.exe listAvailablePackages -repositories source_repository
```

AIX, HP-UX, Linux, and Solaris:

```
./imcl listAvailablePackages -repositories source_repository
```

You should see one or more levels of the offering.

5. Use the `imcl` command to install the product.

Windows:

```
imcl.exe install com.ibm.websphere.WCT.v85_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory installation_directory
-sharedResourcesDirectory shared_directory
-accessRights access_mode
-preferences preference_key=value
-properties property_key=value
-keyring keyring_file -password password
-acceptLicense
```

AIX, HP-UX, Linux, and Solaris:

```
./imcl install com.ibm.websphere.WCT.v85_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory installation_directory
-sharedResourcesDirectory shared_directory
-accessRights access_mode
-preferences preference_key=value
-properties property_key=value
-keyring keyring_file -password password
-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 product.
- 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`.
- You can add a list of tools that are separated by commas—the feature ID `zpm` indicates the Profile Management Tool (z/OS only), `zmm` indicates the z/OS Migration Management Tool, `pct` indicates the Web Server Plug-ins Configuration Tool, and `installtools` indicates the Remote Installation Tool for IBM i.

If a list of features is not specified, the default features are installed.

- The `-accessRights` parameter is not required if you previously specified the mode in which to install Installation Manager.
- 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 Version 1.5 Information Center.

Installing and removing tools in the WebSphere Customization Toolbox

You can use Installation Manager to install or remove a tool in the WebSphere Customization Toolbox.

Before you begin

Make sure that your Installation Manager preferences are pointing to the appropriate Web-based or local repositories containing the WebSphere Customization Toolbox.

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the tool.

About this task

Perform this procedure to use the Installation Manager GUI to install or remove a tool in the WebSphere Customization Toolbox.

Note: Like other Installation Manager operations, you can also invoke a modification using one of the following procedures:

- Using a 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 `imc1` command-line tool
Go to the IBM Installation Manager Version 1.5 Information Center for more information.

Procedure

1. Close the WebSphere Customization Toolbox 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 **WebSphere Customization Toolbox**.
7. Check the appropriate checkbox to install a tool, or clear the appropriate checkbox to remove a tool if you already have it installed.
 - Web Server Plug-ins Configuration Tool
The Web Server Plug-ins Configuration Tool configures the web server plug-ins for WebSphere Application Server so that your web server and application server can communicate with each other.
 - Profile Management Tool (z/OS only)
The Profile Management Tool (z/OS only) creates customized definitions on an Intel-based Windows or Linux operating system that are used to create or augment WebSphere Application Server profiles on z/OS systems. Each customization definition includes a set of customized jobs with associated instructions. The generated jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- z/OS Migration Management Tool

The z/OS Migration Management Tool creates migration definitions on an Intel-based Windows or Linux operating system that are used to migrate a WebSphere Application Server for z/OS node. Each migration definition consists of a set of customized migration jobs with associated instructions. The generated migration jobs must be uploaded to and run on the target z/OS system.

Restriction: This tool can be installed and run on Intel-based Windows and Linux platforms only.

- Remote Installation Tool for IBM i

The `iRemoteInstall` command that is installed when you select this option allows you to install IBM Installation Manager or a WebSphere Application Server product offering from a Windows workstation to a remote target IBM i system. The `iRemoteInstall` command is installed into the following directory:

`wct_root/Remote_Installation_Tool_for_IBM_i`

Restriction: This tool can be installed and run on Windows operating systems only.

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.

Example

In the following list, the optional feature offering names are enclosed in parentheses at the end of the items:

- Web Server Plug-ins Configuration Tool (pct)
- Profile Management Tool (z/OS only) (zpmt)
- z/OS Migration Management Tool (zmmt)
- Remote Installation Tool for IBM i (installtools)

Windows: Here is a response file that modifies an existing WebSphere Customization Toolbox 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.WCT.v85" />
</server>
<uninstall modify='true'>
<offering id='com.ibm.websphere.WCT.v85'
  profile='WebSphere Customization Toolbox V8.5'
  features='zmmt,zpmt' />
</uninstall>
<profile id='WebSphere Customization Toolbox V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox' />
<data key='user.import.profile' value='false' />
<data key='user.select.64bit.image.com.ibm.websphere.WCT.v85' value='false' />
<data key='cic.selector.nl' value='en' />
</profile>
</agent-input>
```

Windows: Here is an example of using the `imcl` command to modify the tools in an installation:

```
imcl.exe modify com.ibm.websphere.WCT.v85
-addFeatures zmmt
-removeFeatures zpmt
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.WCT.v85
-installationDirectory C:\Program Files\IBM\WebSphere\Toolbox
-keyring C:\keyring_file.keyring -password password
```

Installing fix packs on the WebSphere Customization Toolbox using the GUI

You can update the WebSphere Customization Toolbox 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 Version 1.5 Information Center.

About this task

Perform this procedure to use Installation Manager to update the WebSphere Customization Toolbox using the Installation Manager GUI.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on distributed operating systems using the command line
- Uninstalling fix packs from distributed operating systems using the command line

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 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 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, then 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.

4. Click **Next**.
5. Select the version to which you want to update under **WebSphere Customization Toolbox**.
6. Click **Next**.
7. Accept the terms in the license agreements, and click **Next**.
8. Select the tools that you want in your updated installation.
9. 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.
10. Click **Finish**.
11. Click **File > Exit** to close Installation Manager.

Uninstalling fix packs from the WebSphere Customization Toolbox using the GUI

You can roll back the WebSphere Customization Toolbox 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

Perform this procedure to use Installation Manager to roll back the WebSphere Customization Toolbox to an earlier version using the Installation Manager GUI.

Note: For information on installing and removing fix packs for WebSphere Application Server offerings on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- Installing fix packs on distributed operating systems using the command line
- Uninstalling fix packs from distributed operating systems using the command line

Procedure

1. Start Installation Manager.
2. 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.

3. Select the package group to roll back.
4. Click **Next**.
5. Select the version to which you want to roll back under **WebSphere Customization Toolbox**.
6. Click **Next**.
7. 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.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

Uninstalling the WebSphere Customization Toolbox using the GUI

Use the Installation Manager GUI to uninstall the WebSphere Customization Toolbox.

Before you begin

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the WebSphere Customization Toolbox.

If you do not unconfigure existing web server plug-ins that were configured using the Web Server Plug-ins Configuration Tool before uninstalling the WebSphere Customization Toolbox, the configuration information remains. If the WebSphere Customization Toolbox is reinstalled, the configuration information that displays in the Web Server Plug-ins Configuration Tool might be obsolete and greyed out, preventing you from interacting properly with the Web Server Plug-ins Configuration Tool. To resolve this problem, manually remove the workspace used by the previous WebSphere Customization Toolbox installation. The workspace is in the following location:

- *user_home/AppData/Local/IBM/WebSphere/workspaces/WCT8*
- *user_home/.ibm/WebSphere/workspaces/WCT8*

Procedure

1. Start Installation Manager.
2. Click **Uninstall**.
3. In the **Uninstall Packages** window, perform the following actions.
 - a. Select **WebSphere Customization Toolbox** and the appropriate version.
 - b. Click **Next**.
4. Review the summary information.
5. 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.
6. Click **Finish**.
7. Click **File > Exit** to close Installation Manager.

Uninstalling the WebSphere Customization Toolbox using response files

You can uninstall the WebSphere Customization Toolbox using Installation Manager response files.

Before you begin

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the WebSphere Customization Toolbox.

If you do not unconfigure existing web server plug-ins that were configured using the Web Server Plug-ins Configuration Tool before uninstalling the WebSphere Customization Toolbox, the configuration information remains. If the WebSphere Customization Toolbox is reinstalled, the configuration information that displays in the Web Server Plug-ins Configuration Tool might be obsolete and greyed out, preventing you from interacting properly with the Web Server Plug-ins Configuration Tool. To resolve this problem, manually remove the workspace used by the previous WebSphere Customization Toolbox installation. The workspace is in the following location:

- *user_home/AppData/Local/IBM/WebSphere/workspaces/WCT8*
- *user_home/.ibm/WebSphere/workspaces/WCT8*

Optional: Perform or record the installation of Installation Manager and installation of the WebSphere Customization Toolbox 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 the WebSphere Customization Toolbox 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 the WebSphere Customization Toolbox:** On one of your systems, perform the following actions to record a response file that will uninstall the WebSphere Customization Toolbox:

- 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, or Solaris administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/uninstall_response_file.xml
```

- **AIX, HP-UX, Linux, or 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 the WebSphere Customization Toolbox, removing the WebSphere Customization Toolbox 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 Version 1.5 Information Center.

- c. Click **Uninstall**.
 - d. In the **Uninstall Packages** window, perform the following actions.
 - 1) Select **WebSphere Customization Toolbox** 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 the WebSphere Customization Toolbox:** From a command line on each of the systems from which you want to uninstall the WebSphere Customization Toolbox, change to the eclipse/tools subdirectory in the directory where you installed Installation Manager and use the response file that you created to uninstall the WebSphere Customization Toolbox.

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, or Solaris administrator:**

```
./imcl
input /var/temp/uninstall_response_file.xml
-log /var/temp/uninstall_log.xml
```

- **AIX, HP-UX, Linux, or 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 Version 1.5 Information Center for more information.

3. Optional: **List all installed packages to verify the uninstallation.**

Example

The following is an example of a response file for uninstalling the WebSphere Customization Toolbox.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<uninstall modify='false'>
<offering id='com.ibm.websphere.WCT.v85'
  profile='WebSphere Customization Toolbox V8.5'
  features='core.feature,pct,zpmt,zmmt' />
</uninstall>
<profile id='WebSphere Customization Toolbox V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Toolbox'>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\Toolbox' />
<data key='user.import.profile' value='false' />
<data key='user.select.64bit.image.com.ibm.websphere.WCT.v85' value='false' />
<data key='cic.selector.nl' value='en' />
</profile>
</agent-input>
```

Uninstalling the WebSphere Customization Toolbox using the command line

You can uninstall the WebSphere Customization Toolbox using the Installation Manager command line.

Before you begin

Important: When you uninstall the Web Server Plug-ins Configuration Tool, the process does not unconfigure existing web server plug-ins configurations. You might want to use the Web Server Plug-ins Configuration Tool to delete any plug-in configurations that you created using the Web Server Plug-ins Configuration Tool before you remove the WebSphere Customization Toolbox.

If you do not unconfigure existing web server plug-ins that were configured using the Web Server Plug-ins Configuration Tool before uninstalling the WebSphere Customization Toolbox, the configuration information remains. If the WebSphere Customization Toolbox is reinstalled, the configuration information that displays in the Web Server Plug-ins Configuration Tool might be obsolete and greyed out, preventing you from interacting properly with the Web Server Plug-ins Configuration Tool. To resolve this problem, manually remove the workspace used by the previous WebSphere Customization Toolbox installation. The workspace is in the following location:

- *user_home/AppData/Local/IBM/WebSphere/workspaces/WCT8*
- *user_home/.ibm/WebSphere/workspaces/WCT8*

Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Customization Toolbox installation.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.

4. Use the `imc1` command to uninstall the offering.

You can remove a list of tools that are separated by commas—the feature ID `zpm` indicates the Profile Management Tool (z/OS only), `zmm` indicates the z/OS Migration Management Tool, `pct` indicates the Web Server Plug-ins Configuration Tool, and `installtools` indicates the Remote Installation Tool for IBM i. If a list of features is not specified, the entire product is uninstalled.

Go to the IBM Installation Manager Version 1.5 Information Center for more information.

Chapter 7. Preparing the base z/OS operating system

Use this task to prepare your z/OS target systems for WebSphere Application Server for z/OS.

Before you begin

Complete the steps in Chapter 5, “Installing the product on z/OS,” on page 27.

Identify the z/OS systems on which you plan to run WebSphere Application Server for z/OS.

About this task

The WebSphere Application Server for z/OS product makes extensive use of the underlying z/OS operating system services for security, reliability, and performance.

After you install the WebSphere Application Server for z/OS product code, perform the tasks in this section to prepare your z/OS target systems to run WebSphere Application Server for z/OS.

Note: Target systems are the systems on which WebSphere Application Server for z/OS will actually run. The driving system, on which the WebSphere Application Server for z/OS product code installation is performed, might or might not also be a target system.

Procedure

1. Identify the first z/OS target system on which you plan to create a WebSphere Application Server for z/OS application serving environment.
2. Print off a copy of “Checklist: Preparing the base z/OS operating system” on page 75. Use this worksheet to identify which of the following steps have been completed for the target system and record information you will need during product configuration.
3. Prepare z/OS operating system settings. See “Preparing z/OS to run WebSphere Application Server” on page 68 for detailed instructions.
4. Prepare z/OS sysplex settings. See “Preparing the sysplex on z/OS” on page 69 for detailed instructions.
5. Prepare the z/OS job entry subsystem (JES2 or JES3). See “Preparing JES2 or JES3” on page 70 for detailed instructions.
6. Identify TCP/IP resources you want to use and prepare your network. See “Preparing TCP/IP on z/OS” on page 73 for more information.
7. Set up Resource Recovery Services (RRS). See “Preparing Resource Recovery Services (RRS)” on page 71 for more information.
8. Set up your SAF-compliant security package. See “Preparing the security server (RACF)” on page 72 if you will use the z/OS Security Server. If you will use another SAF-compliant security product, consult the product's manufacturer for assistance.
9. If you are using a DB2 database, set up DB2 for concurrency control management.

If your installation uses typical DB2 defaults for U-lock management and lock size, certain WebSphere Application Server applications that use container-managed Enterprise beans (CMP beans) might encounter deadlocks. The likelihood of encountering deadlocks is entirely dependent on the design and execution pattern of the applications. The potential for deadlocks increases with the number and frequency of applications driving concurrent transactions that update the same areas of the DB2 database. If, given the workload for your applications, the potential for deadlocks is high, consider using the following DB2 settings:

RRULOCK(YES)
LOCKSIZE(ROW)

For additional details, see the information about settings for the internal resource lock manager (IRLM) in your DB2 Installation Guide.

Your applications might qualify for the optimistic approach to concurrency control management. To determine whether your applications can use optimistic concurrency control, see the article about concurrency control in the z/OS view of the WebSphere Application Server Information Center.

10. Repeat these steps for each z/OS target system on which you plan to run WebSphere Application Server for z/OS.
11. Keep the worksheets you filled out as you will need some of the information you recorded on them during product configuration.

What to do next

When you have completed this task for each z/OS target system, you are ready to plan your WebSphere Application Server for z/OS application serving environments on these target systems. See Chapter 8, “Planning for product configuration on z/OS,” on page 77 for more information.

Preparing z/OS to run WebSphere Application Server

Procedure

1. Make sure that all software prerequisites listed in “z/OS target system requirements” on page 16 are met.
2. Make sure that the UNIX System Services environment is active and that the BPXPRMxx settings in effect meet or exceed the following minimum values:

```
MAXTHREADS: 10000
MAXTHREADTASKS: 5000
MAXFILEPROC: 10000
MAXSOCKETS (AF_INET domain): 12000
SHRLIBRGNSIZE: 67000000 (134000000 recommended)
```

3. Make sure that each WebSphere Application Server for z/OS server address space, as well as OMVS or batch job address spaces that run Java virtual machines, have access to enough virtual memory below the 2-gigabyte bar. (A Java virtual machine requires at least 250M of virtual memory, for example.) All WebSphere Application Server address spaces should be given at least 1024M of virtual memory.

To do this: Specify REGION=0 (or a suitably large value, such as 1500M) for all batch job, started task and WLM job steps for WebSphere Application Server.

Either specify MAXASSIZE(2147483647) or some similarly large value in BPXPRMxx to provide a large system-wide default address space size for Unix System Services address spaces, or set the ASSIZEMAX value in RACF (or similar security system) for each WebSphere Application Server for z/OS client or server user ID, including IDs used to run the batch Postinstaller or similar processes:

```
ALTUSER WASUTIL1 OMVS(ASSIZEMAX(1073741824)) to allow WASUTIL1 a 1-gigabyte address space
```

4. If you use localization and alternate code pages with UNIX System Services, make sure that all WebSphere Application Server for z/OS server, administrator and client user IDs (any user IDs that run WebSphere Application Server for z/OS scripts) are run with environment variables LANG and LC_ALL both set to the same locale based on code page IBM-1047. Settings based on any other code page can cause the scripts to fail.

See *Changing the Locale in the Shell* in *UNIX System Services User's Guide* for more information.

5. Make sure that the /tmp directory has at least 20 megabytes of free space.

WebSphere Application Server for z/OS makes extensive use of the /tmp directory.

You can use the `df -kP /tmp` shell command to show the number of available 1K blocks in the /tmp directory HFS. Divide the number of available 1K blocks by 1024 to determine the number of megabytes of free space.

If your /tmp directory resides in a permanent read-write HFS, use the **confighfs** command in /usr/lpp/dfsms/bin to extend it as necessary. For example, the following command will add an additional 10 MB of space to the HFS in which /tmp resides:

```
/usr/lpp/dfsms/bin/confighfs -x 10m /tmp
```

If your /tmp directory resides in a temporary file system (TFS), modify the MOUNT statement in BPXPRMxx that defines it to add additional space. To define a 20 MB TFS and mount it at /tmp, for example, use the following MOUNT command:

```
MOUNT FILESYSTEM('/TMP') TYPE(TFS) MOUNTPOINT('/tmp') PARM('-s 20')
```

Note: If you do not specify a space ('-s') value, then the undesirably small default of 1 megabyte will be used.

6. Determine the full dataset names of the following system datasets used by WebSphere Application Server for z/OS:

SCEERUN

Language Environment® runtime library

SCEERUN2

Language Environment runtime library

SIEALNKE

System SSL runtime library

SCLBDLL2

64-bit support code

Also, determine whether these datasets are in the system link pack area (LPA) or link list. Record this information on the worksheet.

7. Make sure that all the following datasets are APF authorized:

- cee_hlq.SCEERUN
- cee_hlq.SCEERUN2
- sys_hlq.SIEALNKE
- clb.SCLBDLL2

8. Make sure that any IEFUSI or JES2/JES3 exits on your system do not restrict WebSphere Application Server for z/OS address spaces to an address space size of less than 512 MB.

Each WebSphere Application Server for z/OS address space should have a region size of at least 512 MB. All WebSphere Application Server for z/OS cataloged procedures are shipped with a default of REGION=0M.

9. Make sure that the TSO segment default region size for WebSphere Application Server for z/OS installer and administrator TSO user IDs is at least 256 MB.

Preparing the sysplex on z/OS

Prepare the sysplex on z/OS.

About this task

WebSphere Application Server for z/OS uses a number of z/OS sysplex services. Therefore, each target system used to run WebSphere Application Server for z/OS must be either a monoplex (single system sysplex) or a member of a sysplex. For more information, see *z/OS MVS Setting Up a Sysplex* (SA22-7625).

Connect systems in a sysplex with channel-to-channel (CTC) communications or through a coupling facility, which is a special logical partition used to share data between sysplex members. Couple datasets on DASD are also used for sysplex coordination.

WebSphere Application Server for z/OS uses the System Logger, an MVS™ component that allows applications to log data in a sysplex, to log error and trace information and provide XA transaction logging. The System logger creates and manages log streams, which are written first to a coupling facility or local in-memory buffer, then transferred to log datasets on DASD for longer term access. Log streams that are written to local buffers rather than to a coupling facility are called DASD-only log streams.

gotcha: If you are using a global resource serialization (GRS) ring to attach one or more monoplexes to a sysplex environment, the cell name of any servers running in any of the monoplexes must be unique within the entire GRS environment. This requirement means that the cell name of a server running in any of the monoplexes:

- Must be different than the cell name of any servers running in the sysplex
- Must be different than the cell name of any servers running in another monoplex that is attached to the sysplex

If you have servers with duplicate cell names within the GRS environment, WebSphere Application Server cannot differentiate between the sysplex cell and the monoplex cell, and treats both servers as part of the same cell. This inaccurate cell association typically causes unpredictable processing results.

Follow these steps to prepare your system for a sysplex.

Procedure

1. Determine if your z/OS target system is already configured as a sysplex.
 - a. If so, continue on to the next step.
 - b. If not, follow the instructions in *z/OS MVS Setting Up a Sysplex (SA22-7625)* to configure it as a monoplex. Record the sysplex name for later use.
2. Determine if System Logger is already in use on your system.
 - a. If so, continue on to the next step.
 - b. If not, follow the instructions in the section *Preparing to Use System Logger Applications in z/OS MVS Setting Up a Sysplex (SA22-7625)*.
3. Decide whether WebSphere Application Server for z/OS log streams should reside in a coupling facility or local in-memory buffers. Record the SMS data class, SMS storage class and dataset name prefix to be used for log datasets. If WebSphere Application Server for z/OS log streams will reside in a coupling facility, choose the structure name to be used.

Preparing JES2 or JES3

Prepare the job entry subsystem on z/OS.

About this task

WebSphere Application Server for z/OS uses job entry subsystem (JES2/JES3) services like any other MVS application.

Procedure

1. Identify the cataloged procedure library or libraries (proclibs) that you will use to hold cataloged procedures for WebSphere Application Server for z/OS. You might need to use separate proclibs for each system in a sysplex.
2. If your system uses JES2 EXIT06 or JES3 IATUX03 to control specification of the REGION= value on JOB or EXEC statements, make sure that this control is relaxed for WebSphere Application Server for z/OS address spaces.

3. If you plan to send WebSphere Application Server for z/OS trace output to the JES spool, make sure you have adequate spool space available. WebSphere Application Server for z/OS address spaces can produce a large number of trace records when tracing is activated.

Preparing Resource Recovery Services (RRS)

WebSphere Application Server for z/OS uses Resource Recovery Services (RRS) to support two-phase transaction commit.

About this task

Note: RRS must be up and running before WebSphere Application Server for z/OS servers are started. See *z/OS MVS Programming: Resource Recovery* (SA22-7616) for more information.

Normally, all systems in a sysplex share a common set of RRS logs for syncpoint processing. If you want to associate specific systems in a sysplex for syncpoint processing, you can specify a log group name when you start RRS. The default log group name is the sysplex name. If you specify a different log group name when you start RRS, it will coordinate syncpoint processing with all systems in the sysplex that use the same RRS log group name.

RRS uses five log streams that are shared by the systems in the log group. Every MVS image that runs RRS needs access to the coupling facility and the DASD on which are defined the system logger log streams for its log group.

Note: You can define RRS log streams as coupling facility log streams or as DASD-only log streams.

If using coupling facility log streams, the RRS images on different systems in a sysplex run independently but share log streams to keep track of the work. If a system fails, an instance of RRS on a different system in the sysplex can use the shared logs to take over the failed system's work.

Use DASD-only log streams only in either single system sysplexes with one RRS image or a sysplex in which information should not be shared among RRS images.

The following list summarizes the RRS logs. In the list, *lgrname* is the log group name. The default log group name is the sysplex name.

ATR.lgrname.ARCHIVE

Information about completed units of recovery (URs). This log stream is recommended but optional.

ATR.lgrname.RM.DATA

Information about the resource managers using RRS services.

ATR.lgrname.MAIN.UR

The state of active URs. RRS periodically moves this information into the RRS delayed UR state log when UR completion is delayed.

ATR.lgrname.DELAYED.UR

The state of active URs when UR completion is delayed.

ATR.lgrname.RESTART

Information about incomplete URs needed during restart. This information enables a functioning RRS instance to take over incomplete work left over from an RRS instance that failed.

In a multiple-system sysplex, RRS log streams should normally reside in a coupling facility.

All RRS transaction logging for WebSphere Application Server for z/OS will occur solely in the DELAYED.UR log stream. You can still configure your MAIN.UR log stream so that it can handle a

production workload in case you deploy a new container or the WebSphere Application Server for z/OS infrastructure changes. WebSphere Application Server for z/OS has no significant impact on the RM.DATA or RESTART logs.

Use the following steps to configure RRS.

Procedure

1. Copy the RRS cataloged procedure, ATRRRS, from SYS1.SAMPLIB to SYS1.PROCLIB (or another proclib in the MSTJCLxx concatenation), and rename it RRS.

If you want, you can set the log group name (GNAME) in the RRS cataloged procedure to a specific value. If you will share the ATRRRS proc among several systems, however, you might prefer to set the log group name at RRS startup or use a system variable in IEASYMxx to set each system's RRS log group name.

2. Establish the dispatching priority of the RRS address space.

The best way to control RRS's dispatching priority is through the workload manager (WLM). IBM recommends that you put RRS in the SYSSTC service class. The service class you choose must give RRS a dispatching priority greater than or equal to the dispatching priority of applications and resource managers that use RRS. SYSSTC will usually accomplish this. For information about system-provided service classes, see *z/OS MVS Planning: Workload Management (SA22-7602)*.

3. Define RRS as a subsystem.

Place the following statement in an active IEFSSNxx parmlib member:

```
SUBSYS SUBNAME(RRS)
```

Place this statement after the statement that defines the primary subsystem. The subsystem name (RRS) must match the name of the RRS cataloged procedure. For more information about IEFSSNxx, see *z/OS MVS Initialization and Tuning Reference (SA22-7592)*.

Note: RRS does not support dynamic subsystem definition, so you cannot use the SETSSI ADD,SUBNAME=RRS command to define RRS as a subsystem. Even though this command will appear to succeed, subsequent attempts to start RRS will fail.

4. Set up the RRS log streams.

5. Start RRS.

- To start RRS with a specific log group name "*lgname*", enter the following MVS console command:

```
START RRS,GNAME=lgname
```

- To stop RRS, enter the following MVS console command:

```
SETRRS CANCEL
```

Note: Do not stop RRS while WebSphere Application Server for z/OS servers are running.

What to do next

For more information on setting up and running RRS, see *z/OS MVS Programming: Resource Recovery (SA22-7616)*.

Preparing the security server (RACF)

Prepare the security server on z/OS.

About this task

WebSphere Application Server for z/OS uses a SAF-compliant security product for its operating system security interfaces. The WebSphere Application Server for z/OS documentation assumes the use of z/OS Security Server (RACF). If you use another security product, consult the vendor for more information.

All z/OS systems in a sysplex must have access to consistent security information--shared RACF database or equivalent. If a shared security database is not used, you are responsible for ensuring that all WebSphere Application Server for z/OS security definitions are in effect on all systems in the sysplex.

Procedure

1. Determine which RACF databases provide security information on your z/OS systems. If any WebSphere Application Server for z/OS cell will run on z/OS systems that have no shared RACF database, make plans to guarantee security database consistency for WebSphere Application Server for z/OS user IDs and privileges.
2. WebSphere Application Server for z/OS requires list-of-groups (GRPLIST) checking. This checking is activated by the WebSphere Application Server for z/OS customization jobs. See *z/OS Security Server RACF Security Administrators Guide* for information about GRPLIST support.
3. In order for RACF to automatically select an unused UID or GID value for WebSphere Application Server User IDs and groups:
 - a. RACF needs to be using application identity mapping at stage 2 or higher. Use the RACF utility IRRIRA00 to upgrade your security database to application identity mapping stage 2 if necessary.
 - b. The RACF profile SHARED.IDS must be defined.
 - c. The RACF profile BPX.NEXT.USER must be defined and used to indicate the ranges from which UID and GID values are to be selected.

For more information, consult the *z/OS Security Server RACF System Programmer's Guide (SA22-7861)* chapter 7, *RACF database utilities*, and the *z/OS Security Server RACF Security Administrator's Guide (SA22-7683)* chapter 20, *RACF and z/OSUnix*.

Preparing TCP/IP on z/OS

Prepare the TCP/IP on z/OS.

About this task

WebSphere Application Server for z/OS follows the CORBA standard, Internet Inter-ORB Protocol (IIOP), for communications. Accordingly, you must consider changes to your TCP/IP network and modify the TCP/IP configuration.

This section provides background information about changes you will need to make to your Domain Name Server (DNS) and TCP/IP. The actual steps to perform are in the customized instructions of the Profile Management Tool and the `zpmmt` command .

Consider the following tips for your TCP/IP network on z/OS.

- You can get started with a simple Domain Name Server (DNS) name server and a single z/OS image, but you should design your initial configuration with growth in mind.

You might, for instance, intend to expand your business applications beyond the monoplex to a full sysplex configuration for performance reasons or to prevent a single point of failure. Several considerations come to bear here.

Several DNS implementations and network router implementations allow the use of a generic location service daemon IP name while dynamically routing network traffic to like-configured servers. If you intend to expand your system beyond a monoplex, it might be worthwhile to use one of these implementations from the start. Non-round-robin DNS name servers limit your ability to expand without retrofitting a name server that allows dynamic network traffic routing.

Recommendation: If you are running in a sysplex, set up your TCP/IP network with Sysplex Distributor. This makes use of dynamic virtual IP addresses (DVIPAs), which increase availability and aid in workload balancing.

Beyond Sysplex Distributor, you have your choice of the following DNS and router implementations on or off z/OS:

- Non-round-robin DNS name servers.
- Round-robin DNS name servers.
- Network routers, such as the IBM Load Balancer. (In previous releases, IBM Load Balancer was known as Network Dispatcher.)
- Select the location service daemon IP name.

For your standalone application server, choose the host name of the server under which you are running. For your deployment manager, choose a generic IP name that can resolve to any or all of the systems where location service daemons run.

You must define the location service daemon host IP name during installation and customization. Use the location service daemon IP name you chose.

Note: The administrative console has a location service daemon configuration page on which you set location service daemon variables.

- Select the port for the location service daemon server.

If you change the location service daemon port number, you can access existing objects after you recycle all your servers. You cannot, however, access the following:

- Any object handles your application stored to disk
- Any object references your application stored in the persistent contexts of the name space.

- Set location service daemon port numbers and IP addresses.

These are initially set using the Profile Management Tool or **zpm** command, but you can subsequently change them in the administrative console. Access the location service daemon configuration page through the administrative console navigation bar (on the left side of screen) under System Administration. If you need to use the IIOp through a firewall, ensure that your firewall supports IIOp.

When recovering a server somewhere other than its configured system, ensure that the same port is not already in use on the system on which it is recovering. If it is, configure the server with a unique port to avoid a conflict.

If comparing WebSphere Application Server for z/OS and WebSphere Application Server for other platforms, realize that only WebSphere Application Server for z/OS has an ORB SSL port.

HTTP and HTTPS ports are found in individual servers under the web container transports, which are in the administrative console as additional properties on the web container configuration page (which is off the server configuration page).

Watch for HTTP transport port conflicts if you previously installed WebSphere Application Server for z/OS.

Ensure that you set up the following port assignments (along with those in the z/OS port assignments chart) on servers that require them in the administrative console:

- ORB port
- ORB SSL port
- Web container transport port
- Web container transport SSL port

See the administrative console and the information center for more information on the WebSphere variables and how to set their values.

You define ports differently depending on whether they are for the first server or subsequent servers. The first server you create is defined, along with its ports, through the Profile Management Tool or the **zpm** command. You have the ability to explicitly specify the ports as you define the server. Subsequent servers and their ports are defined through the administrative console. This means that you define the server first and the ports are automatically assigned. Then, once defined, you can inspect and change the port definitions through the administrative console.

- Some ports, such as the ORB SSL port and the server startup status port, are obtained dynamically.
- Other TCP/IP-related activities include setting up NFS, web server, and Kerberos (which are all optional).

- If you use the DNS on z/OS, you might want to change the refresh timer interval (-t value) associated with the named location service daemon.

The -t value specifies the time (nn, in seconds) between refreshes of cell names and addresses and of the weights associated with those names and addresses. The default is sixty seconds. Reducing the -t value will shorten the lapse time required to register the location service daemon IP name with the DNS, but will also increase DNS processing overhead. In our testing, we used an interval of 10 seconds.

If you use the z/OS DNS, you have to set a location service daemon variable. Do this by setting WebSphere Variable at cell level:

```
daemon_wlmable=1
```

Note: You can perform this for only one cell in a sysplex at a time.

For details, see *z/OS Communications Server: IP Configuration Reference*.

Checklist: Preparing the base z/OS operating system

Print out this worksheet and use it when collecting information about the z/OS system on which you plan to implement WebSphere Application Server for z/OS. Check off each item as you complete the task.

Date: _____

System name: _____

Sysplex name: _____

Preparing z/OS

- _____ Target system hardware and software requirements, including required maintenance in Preventive Service Planning (PSP) bucket, are met.
- _____ UNIX System Services is active with minimum required BPXPRMxx values or better.
- _____ The /tmp directory has at least 20 MB of free space.
- _____ The full dataset names of required system datasets are specified.

Table 4. Dataset names.

Use the following table to specify dataset names of required system datasets.

Item	Dataset name	In LPA or link list?
SCEERUN		
SCEERUN2		
SIEALNKE		
SCLBDLL2		

- _____ System exits (IEFUSI) do not restrict WebSphere Application Server for z/OS address spaces to less than 1024 MB.
- _____ The TSO segment default region size for WebSphere Application Server for z/OS installer and administrator TSO user IDs is at least 512 MB.

Preparing the sysplex

- _____ The target system is configured as a monoplex or into a multisystem sysplex. (Record sysplex name above.)
- _____ System logger is configured.

Table 5. System logger configuration.

Use the following table to specify the system logger configuration.

Should the application servers reside in a coupling facility or DASD-only log streams?	
If a coupling facility, specify the structure name	
SMS data class (for log datasets)	
SMS storage class (for log datasets)	

Preparing JES2 or JES3

- _____ The system proclib for application server cataloged procedures is specified.

Table 6. System proclib for application server cataloged procedures.

Use the following table to specify the system proclib for application server cataloged procedures.

System proclib for application server cataloged procedures	
--	--

- _____ JES2 exit EXIT06 or JES3 exit IATUX03 do not prevent use of REGION= value on JOB or EXEC statements for WebSphere Application Server for z/OS address spaces.
- _____ Spool space is added if necessary.

Preparing Resource Recovery Services

- _____ The RRS cataloged procedure is present in system proclib.

Table 7. RRS cataloged procedure present in system proclib.

Use the following table to specify the RRS cataloged procedure present in system proclib.

Procedure name:	
-----------------	--

- _____ The RRS dispatching priority is set using SYSSTC or other means.
- _____ The RRS cataloged procedure name is defined as a subsystem name in IEFSSN00. The subsystem name must match the cataloged procedure name.
- _____ The RRS log streams are set up.
- _____ RRS starts successfully.

Preparing Security Server (RACF)

- _____ If multiple security databases are in use, a plan is in place to provide database consistency.

Chapter 8. Planning for product configuration on z/OS

This task helps you plan WebSphere Application Server for z/OS application serving environments for your z/OS target systems.

Before you begin

Complete the steps in Chapter 5, “Installing the product on z/OS,” on page 27 and Chapter 7, “Preparing the base z/OS operating system,” on page 67.

Read “WebSphere Application Server for z/OS terminology” on page 78.

About this task

WebSphere Application Server for z/OS uses application-serving environments to provide its functions. Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a practice standalone application server using the default options then proceed to configure the actual product configuration that you want.

Note: The configuration files associated with a WebSphere Application Server runtime environment are called *profiles*. On platforms other than z/OS, profiles can be created, copied, and manipulated using the **manageprofiles** command. In WebSphere Application Server for z/OS, however, all profiles are created using the Profile Management Tool (z/OS only) or the **zpm**t command. With WebSphere Application Server for z/OS, you do not normally need to invoke the **manageprofiles** command or use the **-profile** option on other administrative commands. In fact, creating a profile by running `manageprofiles.sh` directly is not supported on z/OS.

Notes on changes in Version 8:

- When you use the WebSphere Customization Toolbox or **zpm**t.sh command to configure an application server or a management server, note the following changes:
 - The name of the BBOxCPY1 job was changed to BBOxPROC in order to express the function of the customization job more accurately.
 - The BBOxPROC job now must be run after the BBOWWPFx job.

Carefully read and follow the customization instructions generated by the WebSphere Customization Toolbox or **zpm**t.sh command. Do not re-use customization files or data created from a version earlier version of WebSphere Application Server for z/OS.

- In previous versions of IBM WebSphere Application Server for z/OS, certain native (non-UNIX) files were provided in Multiple Virtual Storage (MVS) partitioned datasets such as SBBOJCL. In WebSphere Application for z/OS Version 8.5, these files are distributed in the WebSphere Application Server for z/OS product file system. These files must be exported from the WebSphere Application Server for z/OS product file system into MVS partitioned datasets before they can be used.

Use the **copyZOS.sh** script to export MVS native files into partitioned datasets.

If the dataset does not already exist, it is allocated by the **copyZOS.sh** script. The **copyZOS.sh** script resides in the bin directory of the WebSphere Application Server for z/OS product file system (`/usr/lpp/zWebSphere/V8R5/bin`).

copyZOS file_type data_set_name

Run the **copyZOS.sh** script without options to see a list of supported file types and the required output dataset characteristics for each file type.

Perform the tasks in this section to choose an application serving environment configuration and plan the necessary details for configuration.

Procedure

1. Decide whether to set up a standalone application server or a Network Deployment cell. See “Standalone and Network Deployment configuration differences” on page 99 for more information.
2. Familiarize yourself with “Considerations for WebSphere Application Server for z/OS” on page 82.
3. (Optional) If you have never set up a WebSphere Application Server for z/OS application serving environment before, follow the steps in “Building practice WebSphere Application Server for z/OS cells” on page 115 to gain experience in configuring and working with an application serving environment.
4. Follow the directions for the type of application serving environment you want to configure:
 - “Planning for standalone application server cells” on page 117
 - “Planning for administrative agents” on page 159.
 - “Planning for deployment managers” on page 194.
 - “Planning for Network Deployment cells with application servers” on page 276
 - “Planning for new managed (custom) nodes” on page 228
 - “Planning to federate standalone servers into a Network Deployment cells” on page 264
 - “Planning for job managers” on page 324.
 - “Planning for secure proxy servers” on page 358
 - “Planning for secure proxy administrative agents” on page 387

Use the worksheet included with each option to record your planning decisions and additional configuration information.

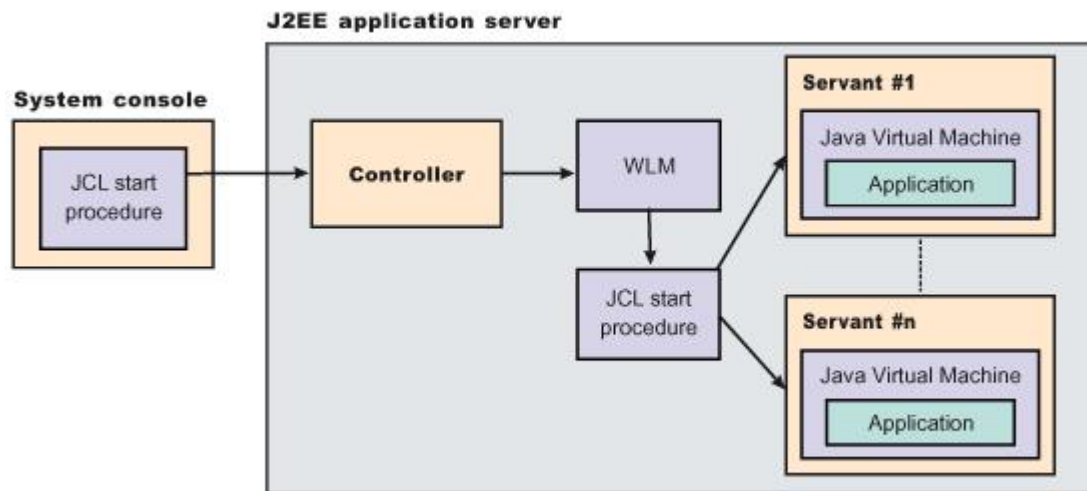
What to do next

When you have completed the planning worksheet for the configuration you have selected, you are ready to configure the application serving environment. See Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 427 for information.

WebSphere Application Server for z/OS terminology

This article describes the z/OS terminology that is required when using WebSphere Application Server for z/OS.

In WebSphere Application Server for z/OS, the functional component on which applications run is a *server*. The following diagram shows a z/OS server running two J2EE applications:



Servers comprise address spaces that run code. A z/OS server has two types of address space: *controllers* and *servants*:

- A controller runs system *authorized* programs and manages tasks, such as communication, for the server. Each server has one controller that you start with a JCL start procedure when you enter the appropriate start command on the MVS console.
- A servant is the address space in which the Java Virtual Machine (JVM) resides. A servant runs *unauthorized* programs such as business applications. A server can have one or more servants running at a time, depending on the workload. When work builds up, Work Load Manager (WLM) dynamically starts additional servants to meet the demand.

Note: The *control region adjunct* (not shown in the diagram) is a specialized servant that interfaces with service integration busses to provide messaging services.

The following types of server can be present on a z/OS system:

Unmanaged (standalone) application server

This application server is set up during standalone configuration to host your J2EE applications.

Managed (Network Deployment) application server

This application server is set up during Network Deployment configuration to host your J2EE applications.

Location service daemon

This server is the initial point of contact for client requests in either standalone or Network Deployment configuration. The location service daemon is a specialized server that have no servants.

JMS server

This server hosts the JMS function in WebSphere Application Server for z/OS, which controls the MQ broker and queue manager in either standalone or Network Deployment configuration. *The JMS server no longer exists as in previous versions of WebSphere Application Server for z/OS. Its function has been replaced with service integration busses.*

Deployment manager

This is a specialized application server that hosts the administrative console application (it hosts only administrative applications) and provides cell-level administrative function in a Network Deployment configuration. The administrative console application administers servers (grouped

into nodes) on many different systems. The deployment manager is the sole occupant of its own node. It does not need a node agent because there are no application servers in the node, and a cell can have only one deployment manager.

Note: The version of the administrative console application that runs in the deployment manager is designed to manage multi-node environments, whereas the version of the administrative console application that runs in the standalone application server is for single node environments only.

Node agent

A node agent provides node-level administrative function in a Network Deployment configuration. A node agent is a specialized server that has no servants.

A node can contain servers that are part of a cluster. The cluster can span nodes if all the involved nodes are in the same cell.

cluster

A cluster is a logical grouping of like-configured servers.

Clusters exist to promote scalability and availability. Workload balancing occurs across the servers in a cluster. Clusters allow you to partition workloads into separate servers while still referring to them as a single unit. Clustering is typically applied to a multinode cell, where each node is configured on a separate system and the cluster has a member (server) on each node. Client requests are distributed among the cluster members based on workload manager decisions.

Note: If you intend your cluster to span multiple systems in a sysplex, you might need to set up a shared HFS.

node A node is a logical collection of servers on one particular z/OS system.

- A node belongs to one cell. The cell to which a node belongs can span several systems, but the node must remain within a single z/OS system.
- A z/OS system can contain multiple WebSphere Application Server for z/OS nodes that belong to the same or different cells.

cell A cell is a logical collection of WebSphere Application Server for z/OS nodes that are administered together. The cell is the largest unit of organization.

- Nodes that comprise a cell can reside on systems in the same sysplex, differing sysplexes, on the same z/OS monoplex, or on differing systems entirely. A cell that consists of nodes on differing systems or sysplexes is called a *heterogeneous* cell.
- A z/OS sysplex or monoplex can contain multiple WebSphere Application Server for z/OS cells.
- Different cells can have nodes on the same systems, although a given node can be a member of only one cell.
- There are two kinds of WebSphere Application Server for z/OS cell:
 - A *standalone* cell consists of a single node. Due to administrative constraints, this node should have only a single application server in it.
 - A *Network Deployment* cell consists of a deployment manager node, which is responsible for cell-wide administrative tasks, and any number of federated nodes. Each federated node contains a node agent, which handles communication with the cell's deployment manager, and any number of application servers.

administrative agent

An administrative agent provides a single interface to administer multiple unfederated WebSphere Application Server for z/OS nodes in environments such as development, unit test, or that portion of a server farm that resides on a single machine.

secure proxy server

A secure proxy server can be installed in the demilitarized zone (DMZ) to reduce the security risk that might occur if you choose to install an application server in the DMZ to host a proxy server.

Every element of the configuration (servers, clusters, nodes and cells) has both a long and short name:

Server name

This is the long name used in the HFS path, and the principal name by which the server is known to WebSphere Application Server for z/OS. It is used to identify the server through the administrative console and scripting. It is a mixed case name and longer than 8 characters.

Server short name

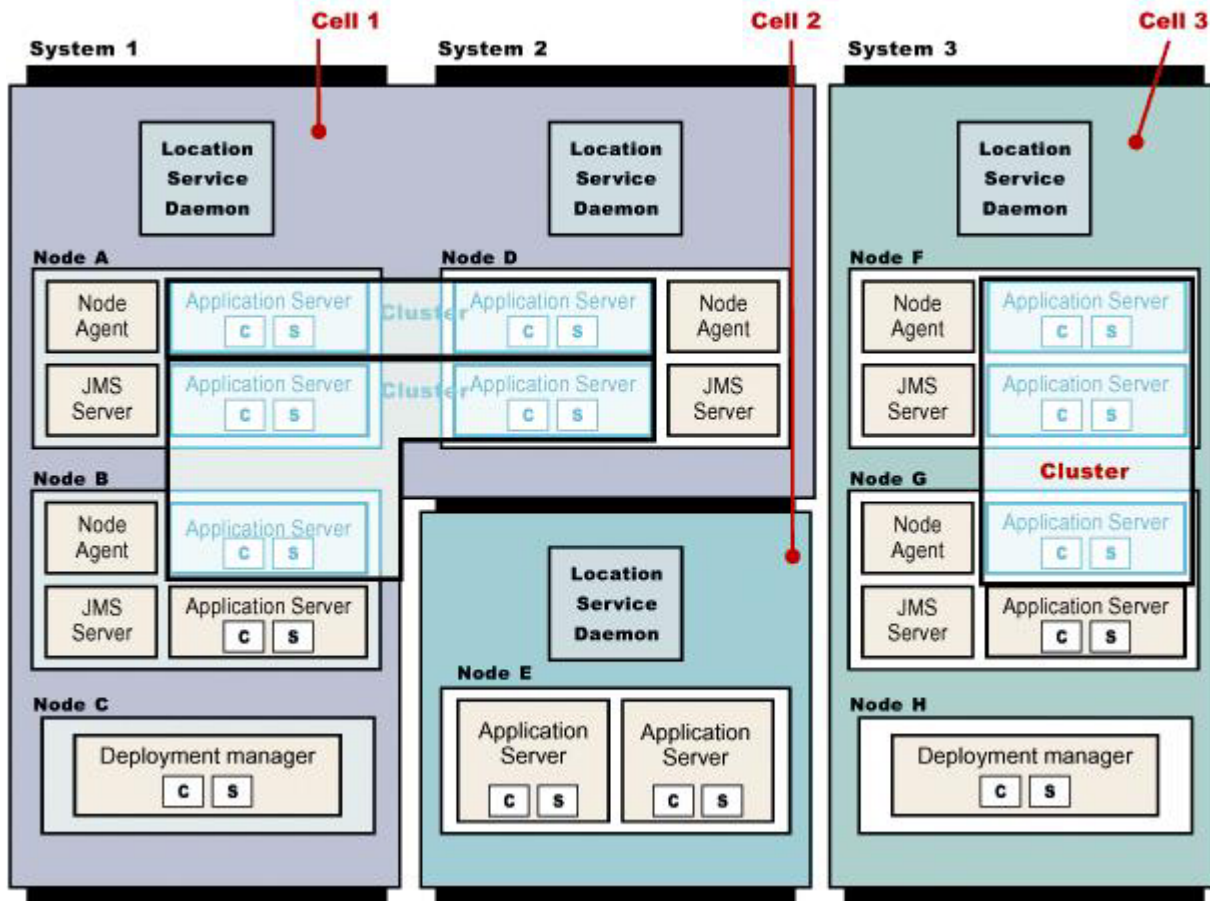
This is the platform-specific native alias, and the principal name by which the server is known to z/OS. It is used to identify the server to underlying z/OS facilities, such as the Security Server, Job Entry Subsystem (JES), WLM and Application Response Management (ARM). For example, the server short name is used as the MVS JOBNAME.

Cluster short name

This is used as the WLM application environment name.

The following diagram illustrates the interaction between servers, clusters, nodes and cells. It shows various configurations that you can set up in a Network Deployment sysplex:

WebSphere for z/OS: Possible configurations in a sysplex



Cells 1 and 3 illustrate Network Deployment configuration cells. Cell 2 is a standalone configuration cell.

Node assignments can vary according to your requirements. The deployment manager node can exist on one system while other nodes that have been federated into the deployment manager can exist on different systems. Such a configured cell comprising differing machines or operating systems is called a *heterogeneous cell* and expands the possible topologies you can consider for your network deployment.

Using a heterogeneous cell to support mixed platforms within a cell

With careful planning, you can manage cells across different z/OS Sysplex and different operating systems.

Cells can span z/OS sysplex environments and spanning other operating systems. For example, z/OS nodes, Linux nodes, UNIX nodes, and Windows nodes can exist in the same Application Server cell. This kind of configuration is referred to as a *heterogeneous cell*.

A heterogeneous cell does require significant planning. The Heterogeneous Cells – cells with nodes on mixed operating system platforms white paper outlines the planning and system considerations required to build a heterogeneous cell.

Considerations for WebSphere Application Server for z/OS

Use this article to familiarize yourself with the z/OS facilities used by the WebSphere Application Server for z/OS application serving environment.

Digital certificates and key rings or key stores are required for Secure Socket Layer communication. These certificates may be stored in the System Authorization Facility (SAF) security database, or in files in the configuration file system.

System Authorization Facility profiles are created during customization to grant necessary authorities to WebSphere Application Server for z/OS address spaces.

Component Trace (CTRACE) facilities in WebSphere Application Server for z/OS are used to manage the collection and storage of trace data. CTRACE data is written to address space buffers in private (pageable) storage, which can be formatted using IPCS if a dump of the address space is taken. CTRACE data can also be written to trace datasets on disk or tape using an external writer. Although CTRACE data is primarily output for use by IBM service personnel, using CTRACE capabilities at your installation allows you to have additional trace data available when a problem first occurs. Because CTRACE efficiently uses system resources, you can collect valuable trace data with minimal impact on performance.

System Logger is used by WebSphere Application Server for z/OS. This is an MVS component that allows applications to log data in a sysplex, to log error and trace information and provide XA transaction logging. The System logger creates and manages log streams, which are written first to a coupling facility or local in-memory buffer, then transferred to log datasets on DASD for longer term access. Log streams that are written to local buffers rather than to a coupling facility are called DASD-only log streams.

System Authorization Facility groups are used by WebSphere Application Server for z/OS to associate user IDs with common sets of permissions.

A common set of SAF groups is used across a WebSphere Application Server for z/OS cell.

A **System Authorization Facility user ID** is associated with each WebSphere Application Server for z/OS address space. (A SAF-compliant security package, such as RACF, is required by the WebSphere Application Server runtime.)

z/OS JCL cataloged procedures

This article describes how WebSphere Application Server for z/OS server uses the JCL cataloged procedures.

Note: During the WebSphere Application Server customization process on z/OS operating systems, the Profile Management Tool (z/OS only) or the `zpmc.sh` command creates a customization job, BBOxPROC, to copy cataloged procedures into your system procedure library. Run the BBOxPROC job so that your server has current cataloged procedures. If you run the WebSphere Application Server for z/OS Version 8.5 code with cataloged procedures from earlier versions, it might result in server startup failures.

Each WebSphere Application Server for z/OS server uses a JCL cataloged procedure. These procedures are all fairly similar and consist of a main cataloged procedure and an INCLUDE member that contains DD statements. Here are sample cataloged procedure library members for a controller as generated by the Profile Management Tool or the `zpmc` command:

Procedure library member BBO8ACR:

```
//BBO8ACR PROC ENV=,PARMS=' ',REC=N,AMODE=00
// SET ROOT='/wasv8config/bbbase/bbonode'
// SET FOUT='properties/service/logs/applyPTF.out'
// SET WSDIR='AppServer'
//*****
/* Test that OMVS can successfully launch a shell and return *
//*****
//TOMVS EXEC PGM=BPXBATCH,REGION=0M,
// PARM='SH exit 13'
//SYSOUT DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWGX)
//SYSPRINT DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWGX)
//*****
/* If the shell RC code is as expected (13) - proceed *
//*****
//IFTST IF (RC = 13) THEN
//*****
/* Start the Multi-Product PTF Post-Installer *
//*****
//APPLY EXEC PGM=BPXBATCH,REGION=0M,
// PARM='SH &ROOT./&ENV..HOME/bin/applyPTF.sh inline'
//SYSOUT DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWGX)
//SYSPRINT DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWGX)
// IF (APPLY.RC <= 4) THEN
//*****
/* If the RC from the Post-Installer is LE 4 then start *
/* the WebSphere Application Server *
//*****
//STEP1 EXEC PGM=BPXBATA2,REGION=0M,TIME=MAXIMUM,MEMLIMIT=NOLIMIT,
// PARM='PGM &ROOT./&WSDIR./lib/s390-common/bbooct1m &AMODE. &PARMS.
//REC=&REC' STDENV DD PATH='&ROOT/&ENV/was.env'
//*
/* Output DDs
//*
//CEEDUMP DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSOUT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSPRINT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//DEFALTD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
// ENDIF
//IFTSTEND ENDIF
```

Procedure library member BBO8ASR:

```
//BBO8ASR PROC ENV=,AMODE=00
// SET ROOT='/wasv8config/bbbase/bbonode'
// SET WSDIR='AppServer'
//STEP1 EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,MEMLIMIT=NOLIMIT,
// PARM='PGM &ROOT./&WSDIR./lib/s390-common/bboosrmr &AMODE.'
//STDENV DD PATH='&ROOT/&ENV/was.env'
//*
/* Output DDs
//*
//CEEDUMP DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSOUT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSPRINT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//DEFALTD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
```

The cataloged procedure specifies where the procedure is processed:

- * EXEC PGM=BPXBATA2,PARM='PGM .../bbooct1m ...' (controller)
- * EXEC PGM=BPXBATSL,PARM='PGM .../bboosrmr ...' (servant)

- * EXEC PGM=BPXBATSL,PARM='PGM .../bboocram ...' (adjunct process)
- * EXEC PGM=BPXBATA2,PARM='PGM .../bbodmnm ...' (location service daemon)

The PARM= parameter on the EXEC PGM statement contains the parameters that are passed to the program identified by the PGM= parameter.

Note: The appropriate interface for making changes to the language environment (LE) parameters is through the was.env file; however, do not modify any LE parameters without first consulting with the IBM Software Support team. The LE parameters are set internally to ensure the best possible performance of the WebSphere Application Server, which is the main LE application running in the address space. If you need to add or change LE parameters, make sure that you work with the IBM Software Support team to ensure that the internally set parameters are not compromised.

The STDENV DD statement points to the was.env (startup parameter) file for the server. The path to this file consists of the configuration HFS directory name (hardcoded using the ROOT JCL variable) and the symbolic link for this particular server, which is specified at startup using the ENV= parameter.

The controller cataloged procedure includes some additional statements before the EXEC statement that invokes BPXBATA2. These are used to invoke the post installer program that applies any needed maintenance to the configuration HFS and its home directories when service is applied to the product HFS and load modules.

The following sections describe the cataloged procedures required for each configuration, provide a recommended naming convention, and explain how the SAF user ID for each server is determined.

Cataloged procedures for standalone application servers

A standalone application server uses the following cataloged procedures:

- Controller cataloged procedure
- Servant cataloged procedure
- Adjunct process cataloged procedure
- Location service daemon cataloged procedure

You can use the same cataloged procedures for different standalone servers if the configuration HFS and product code level (including STEPLIB) are the same for both servers.

Cataloged procedures for Network Deployment cells

A Network Deployment cell uses the following cataloged procedures:

For the deployment manager:

- Deployment manager controller cataloged procedure
- Deployment manager servant cataloged procedure

For each application server node:

- Application server controller cataloged procedure (also used for the node agent)
- Application server servant cataloged procedure
- Adjunct process cataloged procedure

For the location service daemon (one per z/OS system):

- Location service daemon cataloged procedure

The application server servant cataloged procedure is the only one likely to require modification, in order to place libraries (CICS, DB2, and so on) in the STEPLIB concatenation.

You can use the same cataloged procedures for several nodes in a Network Deployment cell, or even for several cells, if the configuration HFS is the same for all of them.

A recommended cataloged procedure naming convention

Use a consistent naming convention for your WebSphere Application Server for z/OS cataloged procedures. The procedure name should distinguish between WebSphere Application Server for z/OS version and configuration HFS

The following convention works for either a standalone application server or Network Deployment cell, for example, where *cc* is a two-character cell identifier:

Procedure	Recommended Name
Deployment manager controller	cc8DCR
Deployment manager servant	cc8DSR
Location service daemon controller	cc8DMN
Application server controller	cc8ACR
Application server servant	cc8ASR
Control region adjunct	cc8AAR

If you require separate cataloged procedures for nodes on different systems in a sysplex (if they need independently settable STEPLIB statements to allow for a nondisruptive restart for example), either place the location service daemon and application server procedures in system-specific proclibs or append a one-character system identifier to the cataloged procedure names for the location service daemon and application servers.

Assigning user IDs to WebSphere Application Server for z/OS address spaces

If you use z/OS Security Server (RACF) as your SAF-compliant security system on z/OS, then STARTED class profiles are used to assign started task user IDs to each WebSphere Application Server for z/OS server. These STARTED profiles are set up by the batch jobs created by the Profile Management Tool or the **zpm** command. Update these STARTED profiles as needed to place servers that you create yourself under the appropriate user IDs.

Controllers (deployment manager, location service daemon, node agent or applications server controller) are started using a console START command that you issue either from the MVS console or internally. For these servers, the STARTED profile name that is checked is of the form *procname.jobname*.

Whenever it creates a controller or daemon cataloged procedure, the Profile Management Tool or the **zpm** command also creates a STARTED profile that associates all controllers using that cataloged procedure with the appropriate controller user ID and configuration group. If you set up a standalone application server with default names, therefore, the Profile Management Tool or the **zpm** command would create the following STARTED profiles for controllers:

- RDEFINE STARTED BB08ACR.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))
- RDEFINE STARTED BB08DMN.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))

Note: TRACE(YES) writes message IRR812I to the MVS console whenever the profile is used.

Servant regions (application server servants and adjunct processes) are started using Workload Manager (WLM). For these servers, the STARTED profile name that is checked is of the form *jobname.jobname*.

Unfortunately, there is no way to assign all servers using a particular servant cataloged procedure to a servant user ID. Therefore, the Profile Management Tool or the **zpm** command creates a STARTED profile

for each servant and one for each control region adjunct. If default names are chosen, the following servant STARTED profiles are created for a standalone application server:

- RDEFINE STARTED BBOS001S.* STDATA(USER(WSSRU1) GROUP(WSCFG1) TRACE(YES))
- RDEFINE STARTED BBOS001A.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))

When you choose cataloged procedure names, make sure that the appropriate STARTED profile is in place to map the server to its appropriate SAF user ID. Use the RACF ISPF panels or the RLIST STARTED command to display the STARTED profiles.

If you use another SAF-compliant security system, contact the security server vendor for WebSphere Application Server for z/OS setup information.

Configuration file systems

There are several planning decisions that you need to make when setting up a WebSphere Application Server for z/OS configuration file system.

Cell, node, and server settings as well as deployed applications are stored in the WebSphere Application Server for z/OS configuration file system. You can use a zSeries file system (ZFS) or hierarchical file system (HFS) for the configuration file system.

Tip: Beginning with WebSphere Application Server for z/OS Version 7.0, the SBBLOAD and SBBOLD2 datasets no longer exist. This is because the load modules are now in the product file system. If you want to switch a configuration from using load modules in the product file system to using load modules in a dataset, you can use the tool described in “switchModules command” on page 534. Beginning with WebSphere Application Server for z/OS Version 8.0, the `server_dlls_in_hfs` environment variable must also be set to 0 for the server to use the DLLs that have been put into a dataset that is in STEPLIB, LPA, or link list. In order for the daemon to pick up the DLLs, `WAS_DAEMON_ONLY_server_dlls_in_hfs` should be set at the cell level.

Each node needs a home directory

Every WebSphere Application Server for z/OS node--whether a standalone application server, deployment manager, managed application server node, or location service daemon--requires a read/write home directory, sometimes referred to as its `WAS_HOME`.

This is the structure of a WebSphere Application Server for z/OS configuration file system, mounted at `/WebSphere/V8R5`. It contains a WebSphere Application Server home directory for a single application server named `BBOS001`, with a cell and a node both named `SYSA`.

```
/WebSphere/V8R5
/AppServer
  /bin
  /classes
  /java
  /lib
  /logs
  /profiles
  /default -> this is the profile_root directory
  /temp
  ...
/Daemon
/config
  /SYSA
  SYSA.SYSA.BBODMNB -> /WebSphere/V8R5/Daemon/config/SYSA/SYSA/BBODMNB
  SYSA.SYSA.BBOS001 ->
/WebSphere/V8R5/AppServer/profiles/default/config/cells/SYSA/nodes/SYSA
/servers/server1
  SYSA.SYSA.BBOS001.HOME -> /WebSphere/V8R5/AppServer
```

The WebSphere Application Server home directory for `BBOS001` is named `AppServer`. It contains directories with complete configuration information for the `SYSA` node and the `BBOS001` server.

The /Daemon directory contains configuration information for location service daemons defined to nodes in this configuration file system.

Note: The /Daemon/config subdirectory is subdivided by cell name. If the cells have different short names, the location service daemon information for each is kept separate.

The daemon home directory has the fixed WebSphere Application Server home name Daemon.

Symbolic links are used to access startup parameters

In addition to the WebSphere Application Server home directories themselves, the configuration file system contains a multipart symbolic link for each server that points to the startup parameters for the server. The symbolic link is named *cell_short_name.node_short_name.server_short_name*.

The sample configuration file system above contains a symbolic link SYSA.SYSA.BBODMNB to start the location service daemon and a symbolic link SYSA.SYSA.BBOS001 to start the BBOS001 application server. The second symbolic link is specified in the ENV parameter on the START command when the server or location service daemon is started from the MVS console:

```
START procname,JOBNAME=BBOS001,ENV=SYSA.SYSA.BBOS001
```

Each symbolic link points to the subdirectory where the server's was.env file resides. This file contains the information required to start the server.

Note: During post-installation processing, described below, the server JCL needs to specify the WebSphere Application Server home directory itself, rather than the location of the was.env file. This is the purpose of the SYSA.SYSA.BBOS001.HOME symbolic link shown above.

Sharing the configuration file system between cells

Two or more WebSphere Application Server for z/OS cells (standalone application server, Network Deployment, or both) can share a WebSphere Application Server for z/OS configuration file system, provided the following conditions are met:

- All cells using the configuration file system must be set up using the same common groups and users. In particular, each must have the same administrator user ID and configuration group.
- The cells must have distinct cell short names.
- Each node must have its own WAS_HOME directory that is not shared with any other node or cell.

As noted above, you can share the daemon home directory (/Daemon) between cells, as it has subdirectories farther down for each cell in the configuration file system.

Note: Be aware that sharing a configuration file system between cells increases the likelihood that problems with one cell might cause problems with other cells in the same configurations file system.

Sharing the configuration file system between systems

Two or more z/OS systems can share a configuration file system, provided the z/OS systems have a shared file system and the configuration file system is mounted R/W. All updates are made by the z/OS system that owns the mount point. For a Network Deployment cell, this is generally the z/OS system on which the cell deployment manager is configured.

Choosing a WebSphere Application Server for z/OS configuration file system mount point

The choice of WebSphere Application Server for z/OS configuration file system mount points depends on your z/OS system layout, the nature of the application serving environments involved, and the relative importance of several factors: ease of setup, ease of maintenance, performance, recoverability, and the need for continuous availability.

- In a single z/OS system:

If you run WebSphere Application Server for z/OS on a single z/OS system, you have a wide range of choices for a z/OS configuration file system mount point. You might want to put several standalone application servers in a single configuration file system with a separate configuration file system for a production server or for a Network Deployment cell. Using separate configuration file system datasets improves performance and reliability, while using a shared configuration file system reduces the number of application server cataloged procedures you need.

You might have one configuration file system with your development, test and quality assurance servers, all in the same common groups and uses as in the following example:

```
/WebSphere/V8R5_test
/DevServer - home to standalone server DVCELL, with server DVSR01A
/TestServer1 - home to standalone server cell T1CELL, with server T1SR01A
/TestServer2 - home to standalone server cell T2CELL, with server T2SR01A
/QAServer - home to Network Deployment cell QACELL, with deployment
manager QADMGR and server QVSR01A
```

and a separate configuration file system for your production cell:

```
/WebSphere/V8R5_prod
/CorpServer1 - home to Network Deployment cell CSCELL, with deployment
manager CSDMGR and server CSSR01A
```

- In a multisystem z/OS sysplex with no shared file system:

In a multisystem sysplex with no shared file system, each z/OS system must have its own configuration file system datasets. For standalone application servers and for Network Deployment cells that do not span systems, the options are the same as for a single z/OS system.

- For Network Deployment cells that span systems:

Here you have two options:

- You can use a different mount point for the cell's configuration file system datasets on each system. This allows you to move nodes easily between systems (if a system becomes inoperative or is being upgraded for example), since each mount point is unused on the other systems in the sysplex, allowing you to mount the failed system's configuration file system datasets on an alternate system in the sysplex.

On system LPAR1, for example, you might have a configuration file system for one part of a cell:

```
/var/WebSphere/V8R5config1
/DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
/AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A
```

with a second configuration file system on LPAR2:

```
/var/WebSphere/V8R5config2
/AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
and F1SR03B
```

This setup has the advantage that you can move the deployment manager and node F1NODEA to LPAR2 or move node F1NODEB to LPAR1. The disadvantage of this configuration is that F1NODEA and F1NODEB will require separate sets of cataloged procedures.

- Or you can use the same mount point for all configuration file system datasets in a particular cell. This allows you to use common cataloged procedures and make the systems look very similar.

Using the same cell setup as above, node LPAR1 would have one configuration file system:

```
/var/WebSphere/V8R5F1
/DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
/AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A
```

and LPAR2 would have a separate file system at the same mount point:

```
/var/WebSphere/V8R5F1
/AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
and F1SR03B
```

However, relocation of either LPAR's node(s) to the other system would require merging a copy of one configuration file system into the other.

- In a multisystem z/OS sysplex with a shared file system:

If your sysplex has a shared hierarchical file system, you can simply mount a large configuration file system for the entire cell. When using the Profile Management Tool or the `zpm` command, specify the common configuration file system mount point on each system. As noted above, you should update the configuration file system from the z/OS system hosting the deployment manager. Performance will depend on the frequency of configuration changes, and ensure you devote extra effort to tuning if this option is chosen.

Alternatively, you can mount a separate configuration file system on each system, perhaps using the system-specific file system mounted at `&SYSNAME` on each system:

```
/LPAR1/WebSphere/V8R5F1
/DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
/AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A

/LPAR2/WebSphere/V8R5F1
/AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
and F1SR03B
```

Each system (LPAR1 and LPAR2) mounts its own configuration file system on its system-specific mount point. When using the Profile Management Tool or the `zpm` command, specify the following:

- `/LPAR1/WebSphere/V8R5F1` on LPAR1
- `/LPAR2/WebSphere/V8R5F1` on LPAR2

Performance is better with this option than with a shared sysplex, and, depending on choice of mount point, it might be possible to mount a configuration file system temporarily on the other LPAR if the original owner is down. You can make cataloged procedures system-specific or use `&SYSNAME` to select the configuration file system mount point.

If you really want to use the same apparent mount point for all configuration file system datasets, you can use symbolic links to redirect a common mount point to a different file system on each system:

- `ln -s $SYSNAME/WebSphere WebSphere`
- Mount LPAR1's configuration file system at `/LPAR1/WebSphere/V8R5F1`.
- Mount LPAR2's configuration file system at `/LPAR2/WebSphere/V8R5F1`.

If this is done correctly, you can specify a configuration mount point of `/WebSphere/V8R5F1` for each system in the Profile Management Tool or the `zpm` command and still enjoy the benefits of system-specific customization file system datasets. However, when this setup is used, it is not possible to easily move configuration file system datasets from one system to another. All nodes expect to find their data in `/WebSphere/V8R5F1`, and you can mount only one configuration file system at this mount point on each system.

- Recommendations:
 - On a single z/OS system, create a read/write file system at `/wasv85config` and use the Profile Management Tool defaults, mounting each configuration file system at `/wasv85config/cell_name/node_name`.
 - On a multisystem sysplex with no shared file system, follow the recommendations above for a single z/OS system. This will allow you to use common cataloged procedures for each cell. Establish separate mount points on each system for any cell that you might need to recover on an alternate system in the sysplex.
 - On a multisystem sysplex with a shared file system, use a shared configuration file system when performance is not an issue or when a shared file system is required to support specific WebSphere Application Server for z/OS functions. Use nonshared configuration file system datasets when performance is an issue, or when you must avoid a single point of failure.

Choosing WebSphere Application Server home directory names

The WebSphere Application Server home directory is always relative to the configuration file system in which it resides. In the Profile Management Tool or the `zpm` command, therefore, you choose the configuration file system mount point on one panel and fill in just the single directory name for the home

directory on another. But when instructions direct you to go to the WAS_HOME directory for a server, they are referring to the entire path name, configuration file system and home directory name combined (/WebSphere/V8R5/AppServer for example).

You can choose any name you want for a home directory if it is unique in the configuration file system. If you are creating a standalone application server or new managed server node to federate into a Network Deployment cell, be sure to choose one that is not in use in the Network Deployment cell's configuration file system.

If you have one node per system, you might want to use some form of the node name or system name. Alternatively, you can use DeploymentManager for the deployment manager and AppServer*n* for each application server node.

Relationship between the configuration file system and the product file system

The configuration file system contains a large number of symbolic links to files in the product file system (/usr/lpp/zWebSphere/V8R5 by default). This allows the server processes, administrator, and clients to access a consistent WebSphere Application Server for z/OS code base.

Note that these symbolic links are set up when the WebSphere Application Server home directory is created and are very difficult to change. Therefore, systems that require high availability should keep a separate copy of the WebSphere Application Server for z/OS product file system and product datasets for each maintenance or service level in use (test, assurance, production, and so forth) to allow system maintenance, and use intermediate symbolic links to connect each configuration file system with its product file system.

Tip: If you configure your Network Deployment environment using the default value for the product file system path in the Profile Management Tool or the `zpm` command, it will result in all the nodes pointing directly at the mount point of the product file system. This makes rolling maintenance in a nondisruptive manner almost impossible. If a cell is configured in this way, applying service to the product file system affects all the nodes at the same time; and if multiple cells are configured in this way, applying service to the product file system affects all the cells at the same time. You might want to specify what is referred to as an intermediate symbolic link between each node's configuration file system and the actual mount point of the product file system. This strategy is described in the WebSphere Application Server for z/OS V5 - Planning for Test, Production and Maintenance white paper. See the WebSphere z/OS V6 -- WSC Sample ND Configuration white paper for more information about this issue and its relationship to applying maintenance. See the WebSphere for z/OS: Updating an Existing Configuration HFS to Use Intermediate Symbolic Links instructions for information on obtaining and using a utility that would allow you to update an existing configuration file system to use intermediate symbolic links.

When a WebSphere Application Server for z/OS node is started, the service level of the configuration is compared against the service level of the product file system. If the configuration file system service level is higher than that of the product file system (probably meaning that an old product file system is mounted), the node's servers will terminate with an error message. If the configuration file system service level is lower than that of the product file system (meaning that service has been applied to the product code base since the node was last started), a task called the post-installer checks for any actions that need to be performed on the configuration file system to keep it up to date.

z/OS logstreams

The z/OS System Logger provides for collections of data called logstreams, which are written to local storage buffers and then to a sysplex coupling facility or DASD for long-term storage. Logstreams can provide high-performance logging for certain applications.

For general information about logstreams, read *z/OS Setting Up a Sysplex* (SA22-7625).

WebSphere Application Server for z/OS can use logstreams for the following types of data:

- Data in the WebSphere Application Server error log, which can be routed to a logstream instead of to a print dataset
- Data in WebSphere Application Server transaction logs, which can be routed to a logstream instead of to a hierarchical file system (HFS) dataset
- Data in WebSphere Application Server Session Initiation Protocol (SIP) recovery logs, which are routed to a logstream

WebSphere Application Server error log

The WebSphere Application Server error log is used to record detailed runtime error and status messages. If the `ras_log_logstreamName` variable is set, error log messages are written to the named z/OS logstream. If the `ras_log_logstreamName` variable is not set or if the named logstream does not exist, error log records are written to `STDERR`.

The primary advantage of sending the WebSphere Application Server error log to a z/OS logstream is that you can consolidate error logs from multiple servers and servant regions. If you place the error logstream in a coupling facility, you can also consolidate error logs from different systems in the same sysplex.

WebSphere Application Server for z/OS provides the following sample jobs to create error logstreams:

BBOERRLC

Create a coupling facility logstream for the WebSphere Application Server error log

BBOERRLD

Create a DASD-only logstream for the WebSphere Application Server error log

Use the `copyZOS.sh` script to write these jobs to a partitioned dataset.

After you create the logstream, use scripting or the administrative console to set the `ras_log_logstreamName` variable to the logstream name for all servers whose output is to go to the newly created logstream.

Use the `BBORBLOG` script in the `SBBOEXEC` profile dataset to view the error log. Read the *Viewing error log contents through the Log Browse Utility* article in the information center for more information.

Transaction XA partner log

The WebSphere Application Server transaction XA partner log is used to record transaction (JTA) information. This information is written to an HFS file or a z/OS logstream, depending on the setting of the transaction directory file for a specific server:

- If the transaction directory value is `dir://directory_name`, the named file system directory is used for storing transaction information.
- If the transaction directory value is `logstream://logstream_name`, transaction information is written to the named logstream.

The default is `dir://app_server_root/tranlog/server_name`.

By using a z/OS logstream for the WebSphere Application Server transaction log and placing that logstream in a coupling facility, you can improve performance for cross-system restart operations.

WebSphere Application Server for z/OS provides the following sample jobs in the `SBBOJCL` product dataset to create transaction logstreams:

BBOTXALC

Create a coupling facility logstream for a WebSphere Application Server transaction log

BBOTXALD

Create a DASD-only logstream for a WebSphere Application Server transaction log

Use the copyZOS.sh script to write these jobs to a partitioned dataset.

After you create the logstream, use the administrative console to set an individual server's transaction log to `logstream://logstream_name` on the configuration tab of the server's transaction service settings (**Servers > Server Types > WebSphere application servers > server_name > Container Services > Transaction Service**) and restart the server. Read the *Transaction service settings* article in the information center for more information.

Note: When an application server is federated into a Network Deployment cell, you must clear any existing transaction errors. If transaction logging is being done to a z/OS logstream, delete the server's transaction logstream after the application server is shut down and recreate it before starting the newly federated application server.

Creating SIP recovery logstreams

If your Network Deployment cell configuration includes replication partners across several LPARs, SIP recovery logstreams must reside in a coupling facility. DASD recovery logstreams can be used only if all replication partners are on the same LPAR.

SIP logstreams must follow a very specific pattern for their names: `CELL_NAME.SERVER_NAME.D` and `CELL_NAME.SERVER_NAME.M`.

You might experience errors that indicate that a logstream is full or corrupted. In this situation, you might need to delete and redefine the logstream. The following examples show jobs that can be used to perform these actions:

Delete the logstream:

```
//DEFLOGA JOB MSGLEVEL=(1,1),MSGCLASS=H,NOTIFY=&SYSUID,REGION=0M
/**
//LOGDEFN EXEC PGM=IXCMIAPU,REGION=4M
//SYSPRINT DD SYSOUT=*
/**
//SYSIN DD *
DATA TYPE(LOGR)
DELETE LOGSTREAM
NAME(WTOCELL.WT0S000.M)
DELETE LOGSTREAM
NAME(WTOCELL.WT0S000.D)
DELETE LOGSTREAM
NAME(WTOCELL.WT0S001.M)
DELETE LOGSTREAM
NAME(WTOCELL.WT0S001.D)
/*
```

Recreate the logstream:

```
//DEFLOGA JOB MSGLEVEL=(1,1),MSGCLASS=H,NOTIFY=&SYSUID,REGION=0M
/**
//LOGDEFN EXEC PGM=IXCMIAPU,REGION=4M
//SYSPRINT DD SYSOUT=*
/**
//SYSIN DD *
DATA TYPE(LOGR)
DEFINE LOGSTREAM
NAME(WTOCELL.WT0S000.M)
DASDONLY(YES)
HLQ(LOCAL) MODEL(NO)
LS_SIZE(2048)
STG_SIZE(2048)
LOWOFFLOAD(60)
HIGHOFFLOAD(80)
DEFINE LOGSTREAM
NAME(WTOCELL.WT0S000.D)
DASDONLY(YES)
HLQ(LOCAL) MODEL(NO)
LS_SIZE(2048)
STG_SIZE(2048)
LOWOFFLOAD(60)
```

```

HIGHOFFLOAD(80)
DEFINE LOGSTREAM
NAME(WT0CELL.WT0S001.M)
DASDONLY(YES)
HLQ(LOCAL) MODEL(NO)
LS_SIZE(2048)
STG_SIZE(2048)
LOWOFFLOAD(60)
HIGHOFFLOAD(80)
DEFINE LOGSTREAM
NAME(WT0CELL.WT0S001.D)
DASDONLY(YES)
HLQ(LOCAL) MODEL(NO)
LS_SIZE(2048)
STG_SIZE(2048)
LOWOFFLOAD(60)
HIGHOFFLOAD(80)
/*
//

```

Output destinations

Various server DD statements are used to address system output such as, console output, trace output, and dump output.

Since WebSphere Application Server controllers and servants are z/OS started task address spaces, they can produce a variety of output:

- Server output and error messages
- Trace records
- System dumps

This output can be written to a variety of destinations:

- JES2 print and punch files (referred to as STDERR or job output)
- Files written to the configuration file system or other file systems
- z/OS log streams
- Component trace datasets

Reusable address space

The z/OS operating system assigns an *address space ID (ASID)* when it creates each address space. However, a limited number of ASIDs are available for the operating system to assign. When all ASIDs are assigned to existing address spaces, the operating system is unable to start a new address space. In this situation, the operating system issues the IEA602I ADDRESS SPACE CREATE FAILED message.

In some scenarios, address spaces that use cross-memory services prevent their ASIDs from being reused and increase the possibility of an ASID shortage. One solution, which became available in Version 1.9 of the z/OS operating system, is to explicitly indicate that specific address spaces can use reusable ASIDs. This article describes the use of reusable ASIDs by WebSphere Application Server on the z/OS operating system.

Before using the Reusable ASID feature

The reusable ASID feature is activated on a particular z/OS system when you specify REUSASID(YES) in PARMLIB member DIAGxx. If you do not specify this parameter, the reusable ASID feature is not used. If you are using Version 1.9 of the z/OS operating system, you must apply the Workload Manager (WLM) APAR OA28528.

All code that is running in reusable address spaces, such as MVS exits, must comply with the ASID reuse rules that are outlined in the z/OS Extended Addressability Guide. Otherwise, problems that are like the one described in OA28528 might abend the address space.

Running started tasks in reusable address spaces

To indicate that a started task using cross-memory services can run in a reusable address space, specify the REUSASID=YES option on the **START** command for the started task. For example:

```
START STC1,REUSASID=YES
```

Important: This command is not effective unless you activate the REUSASID feature in parmlib member DIAGxx.

Avoid specifying the REUSASID option for started tasks that do not use cross-memory services. This approach is not recommended because reusable ASIDs form a separate pool that is not available for reassignment to an ordinary address space.

If you use the MVS **START** command to start WebSphere Application Server for z/OS controllers or location services daemons directly, you must add the REUSASID option if you want them to run in reusable address spaces. For example:

```
START BB06ACR,JOBNAME=BBOS001,ENV=BB0BASE.BBONODE.BBOS001,REUSAID=YES
START BB06DMN,JOBNAME=BBODMNC,ENV=BB0CELL.CFCIMGWI.WITIMGWI,REUSASID=YES
```

WebSphere Application Server address spaces also can be issued by WebSphere Application Server itself. For example, the address spaces might be issued when the location service daemon starts automatically or when a server starts with the **startServer** command. In these cases, the daemon or server configuration settings determine whether the REUSASID=YES option is specified on the **START** command that is submitted by WebSphere Application Server.

By default, the location service daemon always starts with the REUSASID=YES option when WebSphere Application Server issues the **START** command.

For other servers, by default, each controller starts with the REUSASID=YES option. You can change this behavior by manually updating the process definitions for the controller. To make the update, use either the wsadmin command, or scripting, to remove or include the REUSASID option on the server **START** command. Also, you can use the updateZOSStartArgs script to add or remove the REUSASID=YES option for particular servers.

Note:

- WebSphere Application Server servant regions and control regions adjuncts do not normally run in reusable address spaces.
- Bindings mode WebSphere MQ connectors do not work properly in reusable address spaces. If you activate reusable ASIDs on your z/OS operating system, ensure that servers that are running with Message Listener Ports, as opposed to activation specifications, do not have the REUSASID=YES option on the **START** commands.

For more information about reusable address spaces, see the z/OS manual MVS Programming: Extended Addressability Guide.

Scheduler database

This concept describes the scheduler service in WebSphere Application Server and the timing intervals.

The scheduler service in WebSphere Application Server is responsible for starting actions at particular times or intervals. The performance of the scheduler database is critical to efficient scheduler operation.

WebSphere Application Server for z/OS provides the following sample jobs in the SBBOJCL product dataset to create a local scheduler database using DB2:

BBOCRTTS

Create DB2 table spaces for a scheduler database

BBOCRTSC

Create DB2 schemas for a scheduler database

=

The following sample jobs in SBBOJCL can be used to delete a scheduler database in DB2 when it is no longer needed:

BBODRPSC

Drop DB2 schemas for a scheduler database

BBODRPTS

Drop DB2 table spaces for a scheduler database

Make copies of these jobs, customize them according to the instructions in the job, and run as needed to create or delete scheduler databases.

Read the *Using schedulers* article for information on using a scheduler.

Port number settings on z/OS

This article lists the default server values for WebSphere Application Server for z/OS.

z/OS port assignments

Table 8. Port definitions for WebSphere Application Server for z/OS. The table lists port names and the default values of the port numbers.

Port Name	Default Value							
	Standalone Application Server	Federated Application Server	Deployment Manager	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Server Administrative Agent	Administrative Subsystem
Administrative Console Port (WC_adminhost)	9060	----	9060	9060	9960	----	----	----
Administrative Console Secure Port (WC_adminhost_secure)	9043	----	9043	9043	9943	----	----	----
HTTP Transport Port (WC_defaulthost)	9080	9080	----	----	----	80	----	----
HTTPS Transport Secure Port (WC_defaulthost_secure)	9443	9443	----	----	----	443	----	----
ORB Listener Port (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)	2809	2809	9809	9807	9808	----	9807	----

Table 8. Port definitions for WebSphere Application Server for z/OS (continued). The table lists port names and the default values of the port numbers.

Port Name	Default Value							
	Standalone Application Server	Federated Application Server	Deployment Manager	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Server Administrative Agent	Administrative Subsystem
Cell Discovery Port (CELL_DISCOVERY_ADDRESS)	----	----	7277	----	----	----	----	----
High Availability Manager Communication Port (DCS_UNICAST_ADDRESS)	9353	9353	9352	----	----	----	----	----
Internal JMS Server Port (JMSSERVER_SECURITY_PORT)	5557	----	----	----	----	----	----	----
Administrative Interprocess Communication Port (IPC_CONNECTOR_ADDRESS)	9633	9633	9632	9630	9631	9633	9630	9634
MQ Transport Port (SIB_MQ_ENDPOINT_ADDRESS)	5558	5558	----	----	----	----	----	----
MQ Transport Secure Port (SIB_MQ_ENDPOINT_SECURE_ADDRESS)	5578	5578	----	----	----	----	----	----
ORB SSL Listener Port (ORB_SSL_LISTENER_ADDRESS)	0	0	0	0	0	----	----	----
RMI Connector Port (RMI_CONNECTOR_ADDRESS)	----	----	----	----	----	----	----	9810
JSR 160 RMI Connector Port (JSR160RMI_CONNECTOR_ADDRESS)	----	----	----	----	----	----	----	9811
Service Integration Port (SIB_ENDPOINT_ADDRESS)	7276	7276	----	----	----	----	----	----
Service Integration Secure Port (SIB_ENDPOINT_SECURE_ADDRESS)	7286	7286	----	----	----	----	----	----

Table 8. Port definitions for WebSphere Application Server for z/OS (continued). The table lists port names and the default values of the port numbers.

Port Name	Default Value							
	Standalone Application Server	Federated Application Server	Deployment Manager	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Server Administrative Agent	Administrative Subsystem
SIP Container Port (SIP_DEFAULTHOST)	5060	5060	----	----	----	5060	----	----
SIP Container Secure Port (SIP_DEFAULTHOST_SECURE)	5061	5061	----	----	----	5061	----	----
JMX SOAP Connector Port (SOAP_CONNECTOR_ADDRESS)	8880	8880	8879	8877	8876	----	8877	8881
DataPower® Appliance Manager Secure Inbound Port (DataPowerMgr_inbound_secure)	----	----	5555	----	----	----	----	----
Middleware Agent RPC Port (XDAGENT_PORT)	----	----	7060	----	----	----	----	----
Administration Overlay UDP Port (OVERLAY_UDP_LISTENER_ADDRESS)	11003	11003	11005	----	----	----	----	----
Administration Overlay TCP Port (OVERLAY_TCP_LISTENER_ADDRESS)	11004	11004	11006	----	----	----	----	----
Status Update Listener Port (STATUS_LISTENER_ADDRESS)	----	----	9420	----	9425	----	----	----
IBM HTTP Server Port	80	----	----	----	----	----	----	----
IBM HTTPS Server Administration Port	8008	----	----	----	----	----	----	----

When you federate an application server node into a deployment-manager cell, the deployment manager instantiates the node agent server process on the application server node. The node agent server uses these port assignments by default.

Table 9. Port definitions for the node agent server process. The table lists port names and the default values of the port numbers.

Port Name	Default Value
	Cell Node Agent
JMX SOAP Connector Port (SOAP_CONNECTOR_ADDRESS)	8878
ORB Listener Port (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)	2810
High Availability Manager Communication Port (DCS_UNICAST_ADDRESS)	9354
ORB SSL Listener Port (ORB_SSL_LISTENER_ADDRESS)	0
Node Discovery Port (NODE_DISCOVERY_ADDRESS)	7272
Node Multicast Discovery Port (NODE_MULTICAST_DISCOVERY_ADDRESS)	5000
Node IPv6 Discovery Port (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)	5001
Node Agent Interprocess Communication Port (IPC_CONNECTOR_ADDRESS)	9626
Node Middleware Agent RPC Port (NODE_XDAGENT_PORT)	7061
Node Administration Overlay UDP Port (NODE_OVERLAY_UDP_LISTENER_ADDRESS)	11001
Node Administration Overlay TCP Port (NODE_OVERLAY_TCP_LISTENER_ADDRESS)	11002

Location service daemon ports

Standalone application server node location service daemons are considered temporary. The ports assigned to a standalone application server node's location service daemon are used only until that node is federated. It is advisable to set aside a couple of ports to serve as interim ports for the standalone application server node location service daemon. The permanent location service daemon ports are the ones assigned to the deployment manager. Those same ports are copied to location service daemons created when a standalone application server node on another MVS image is federated into the deployment manager cell.

Node agent ports

There is a node agent per MVS image on which the cell spans. One design option calls for all node agents to have the exact same ports so the Sysplex Distributor is able to balance the traffic between the two. The node agent is created when the BBOWADDN customized job is run.

Server clusters

A server cluster is a grouping of two or more servers into a one logical server. A cluster is created through the administrative console. Servers within a cluster are called cluster members. Servers (members) within a cluster start out being clones of one another. When it comes to the TCP ports for the members in a cluster, the administrative console allows you during the creation of the cluster to specify if you want the HTTP ports to be unique or the same. The other ports -- bootstrap, ORB, ORB SSL and SOAP -- will be made unique by the application server.

For complex configurations with multiple members in a cluster it is advisable to make the members be as nearly identical to one another as possible, including the TCP ports. Therefore, when planning it is recommended a range of ports be allocated for a cluster with the intention to make certain all members of that cluster were given the same set of ports. Because WebSphere will automatically generate unique ORB, ORB SSL and SOAP ports for the second cluster member, it is necessary to go back in and remap the ports back to the ports set aside for the server cluster

Note: When a vertical cluster, two members on the same MVS image, is the potential configuration, you will need to consider port sharing by two members of the same cluster on the same MVS image.

z/OS workload management (WLM)

This concept is an explanation of how WebSphere Application Server for z/OS uses the workload management (WLM) function of z/OS to start and manage servers in response to workload activity.

Each Java EE application server in a WebSphere Application Server for z/OS cell uses WLM to start servants as WLM application environments. Thus, each application server must be associated with a WLM application environment name. The Cluster transition name in the WebSphere Application Server for z/OS configuration is used as the WLM application environment name.

Standalone and Network Deployment configuration differences

A table is presented that contains specifics on the differences between a WebSphere Application Server for z/OS standalone cell and Network Deployment cell.

Table 10. Standalone and Network Deployment configuration differences.

The following table describes the differences between a WebSphere Application Server for z/OS standalone cell and Network Deployment cell.

	Standalone cell	Network Deployment cell
Configuration:	Set up each standalone server node through the Profile Management Tool or the <code>zpm</code> command. Set up additional servers within the node through the administrative console or scripting.	Set up each deployment manager node through the Profile Management Tool or the <code>zpm</code> command. Add application server nodes to the Network Deployment cell through the Profile Management Tool or the <code>zpm</code> command.
Address spaces:	Minimum: four (location service daemon, controller, servant, control region adjunct)	Minimum: seven (location service daemon, application server controller, application server servant, application server control region adjunct, deployment manager controller, deployment manager servant, node agent)
	Maximum: Limited only by resources.	Maximum: Limited only by resources.
Administrative isolation:	Each standalone server node is a separate administrative domain.	All nodes in the cell are in the same administrative domain.
Operational isolation:	You can start and stop servers independently. Each server has an independent, unshared JNDI namespace.	You can start and stop servers independently. The JNDI namespace is shared among all servers in the cell.
Application servers allowed to have multiple servants?	Yes	Yes
Clustering available?	No	Yes

z/OS application server naming conventions

There are several names that you must specify during WebSphere Application Server for z/OS configuration. Although it is possible to assign names to WebSphere Application Server for z/OS objects on an ad-hoc basis, it is safer and more efficient to assign names in an orderly fashion.

Long names and short names

Each WebSphere Application Server for z/OS cell, node, server, and cluster must have both a long name and a short name.

Long names

Long names are the principal names by which cells, nodes, servers, and clusters are known to WebSphere Application Server for z/OS. These are the names used in scripting and the administrative console. Long names can be up to 50 characters long and include mixed-case alphabetic characters, numeric characters, and the following special characters: ! ^ () _ - . { } []

Short names

Short names are specific to the z/OS implementation of WebSphere Application Server and are the principal names by which cells, nodes, servers, and clusters are known to z/OS.

Note: The z/OS operating system has an eight-character limit on many operating-system interface values.

Short names must be from one to eight characters long, can contain only uppercase alphabetic or numeric characters, and cannot begin with a numeric character.

You should limit your server short names to seven characters to allow the runtime to add an S or an A to a short name to designate servant regions or adjuncts. For example, a server short name of BBOS001 results in BBOS001S for servant regions and BBOS001A for control region adjunct processes. If your standards require eight characters for server short names, explicitly set the short names of the servant and adjunct regions.

Wherever this article states that two names must be the same or different, this means that the long names must be the same or different and that the short names must also be the same or different. There is no requirement that the long and short names be related, but most users find it convenient to make them identical or at least similar to each other.

Choosing a cell name

The cell name identifies a WebSphere Application Server cell. Each of the following is a cell:

1. Standalone application server
2. Network Deployment cell, together with its nodes and servers
3. DMZ secure proxy server
4. Administrative agent
5. Job manager

Each cell must have cell name that it does not share with any other cell on the same system. If cells on different systems communicate with one another, they should not have the same cell name.

In order to federate a standalone application server into a Network Deployment cell, the standalone server's cell name must be different from the cell name of the Network Deployment cell.

Choosing a server name

The server name identifies a WebSphere Application Server server within the node to which it belongs. Each server must have server name that it does not share with any other server in the same node. On the z/OS operating system, the server short name is also used as the server's MVS job name; and therefore, no two servers with the same server short name can run on the same z/OS system at the same time even if they are in different cells.

Standalone application servers

A standalone application server usually has a single application server because the administrative console in a standalone application server cell can only control a single server. If the application server node is registered with an administrative agent, however, the administrative agent can be used to create additional servers.

Network Deployment cells

A Network Deployment cell has at least one server—the deployment manager in its own node—and some number of additional application servers, web servers, proxy servers, and other types of servers.

Secure proxy servers, administrative agents, and job managers

Secure proxy servers, administrative agents, and job managers each have a single server.

Choosing cluster names and generic server short names

The cluster name identifies a WebSphere Application Server cluster—a collection of identical servers, potentially spanning several nodes or systems, that run the same applications. Both application servers and proxy servers can be clustered. Each cluster must have cluster name that it does not share with any other cluster in the same cell.

The cluster short name has a special function—it is used to identify the cluster servers to the z/OS Workload Management facility (WLM). Even nodes that have not been clustered have a server generic short name, also called a cluster transition name, that is used for the same purpose; when a cluster is created from an existing application server, the server's generic short name becomes the cluster name.

As a result, no two servers on the same z/OS system should have the same server generic short name unless they are in the same cluster. This rule applies to deployment managers, node agents, administrative agents, and job managers as well as to application servers and proxy servers.

Naming conventions

Because of the large number of names to be chosen, together with the requirements that some names be the same or be unique, it is helpful to have a standard method of choosing names that meets both the enterprise's business needs and the requirements of the WebSphere Application Server architecture.

WebSphere Application Server for z/OS provides two different naming conventions for cells, nodes, servers, and clusters.

Basic naming convention

This convention includes a set of fixed defaults that have been in place since WebSphere Application Server for z/OS Version 4.0 with some adjustments to allow for new server types in Version 7.0 and later. These defaults are intended for getting started with WebSphere Application Server on z/OS, and they only support a single server of each type on a given z/OS system. Additional servers require that the default values be changed.

Read “z/OS basic naming convention” for more information on this naming convention.

Standard naming convention

This convention includes a set of structured defaults that use names generated from one- or two-character cell, cluster, and system identifiers that you choose during customization. These defaults support arbitrary numbers of cells, nodes, and servers; and they are intended for production environments.

Read “z/OS standard naming convention” on page 107 for more information on this naming convention.

You can develop your own naming convention, but it should take into account the considerations discussed in this article and described in more detail in the related articles on the basic and standard naming conventions.

z/OS basic naming convention

In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the `zpm` command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Fixed defaults are used that follow the basic naming convention if one- and two-character cell, cluster, and system identifier values are not specified during customization.

The basic naming convention is intended to assist you in gaining experience with WebSphere Application Server on z/OS, and it is suitable for small application environments consisting of a single application

server or Network Deployment cell with one each of the other types of servers—administrative agent, job manager, and secure proxy server. If a Network Deployment cell is created, additional servers can be generated in the single application server node.

Default values for a standalone application server

By default, a standalone application server is build with cell short name BBOBASE, node short name BBONODE, and server short name BBOS001. The corresponding long names are cell name bbobase, node name bbonode, and server name server1. This illustrates the convention that the default long names are simply the lowercase forms of the corresponding short names, which only use uppercase letters, unless there is a traditional name such as server1 or proxy1 that is used instead. The server generic short name, which is used to identify the server to Workload Management, is BBOC001.

The default dataset name for the configuration file system is the following:

OMVS.WAS85.BBOBASE.BBONODE.HFS
(or .ZFS if a zFS file system is selected)

and it is mounted at the following location:

/wasv8config/bbobase/bbonode

This shows another feature of both the basic and standard naming conventions in WebSphere Application Server for z/OS Version 8.5. The cell and node short names are used to name the configuration file system and this file system's mount point is based on the cell and node long names. This convention helps to familiarize installers with the relevant names in each cell and makes it easy to remount file systems in the appropriate places.

Table 11. SAF groups and user IDs.

The following SAF groups and user IDs are created during customization:

WSCFG1	Configuration group Provides administration and server privileges
WSSR1	Servant group Provides privileges needed by servant regions
WSCLGP	Unauthenticated, local user, or guest group Provides basic privileges to access the cell but nothing more
WSCRUI	Controller user ID Controller, control region adjunct, and daemon started tasks
WSSRU1	Servant user ID Servant started tasks
WSADMIN	Administrator user ID Used for cell configuration and, in certain circumstances, as a WAS administrator
WSGUEST	Unauthenticated-user user ID (z/OS-managed security only) Represents an unknown user for security purposes

Table 12. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOS001	BBO8ACR	Controller
BBOS001A	BBO8AAR	Control region adjunct (handles messaging tasks for the controller)
BBOS001S	BBO8ASR	Servant region
BBODMNB	BBO8DMNB	Location service daemon

Note that the cataloged-procedure names in the second column of this table provide the following:

- Product indication (BB0)
- Product version number (8)
- Indication of the type of server (A for application server)
- Two characters showing the started task type (CR for controller, AR for adjunct region, and SR for servant region)

This pattern is used throughout the basic naming convention. The daemon job name and cataloged-procedure names follow their own pattern.

Default values for a deployment manager

To build a Network Deployment cell, you start with a deployment manager. To allow a standalone application server that is also built with the defaults to be federated into the Network Deployment cell, you must choose a new cell name and node name for the deployment manager.

By default, a deployment manager is built with cell short name BBOCELL, node short name BBODMGR, and server short name BBODMGR. The corresponding long names are cell name `bboce11`, node name `bbodmgr`, and server name `dmgr`. The deployment manager long name is fixed by the product architecture. The deployment manager can never be clustered; therefore, its default server generic short name, which is used to identify the deployment manager to Workload Management, is the same as the server short name: BBODMGR.

In versions of WebSphere Application Server for z/OS earlier than Version 7.0, the z/OS system name and sysplex name were used as cell names for the standalone application server and Network Deployment cell, respectively. This limited the old naming convention to a maximum of two cells for one z/OS system. In addition, there is no reason for a z/OS system name and its sysplex name to be different, causing a collision if the two values are used as names for different cells. In WebSphere Application Server for z/OS Version 7.0 and later, fixed cell names are used to avoid these problems.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS85.BBOCELL.BBODMGR.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv8config/bboce11/bbodmgr
```

The SAF groups and user IDs created during customization have the same default names as for the standalone application server in order to make federation possible and minimize the number of security database entries that must be created.

Table 13. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBODMGR	BBO8DCR	Controller
BBODMGRS	BBO8DSR	Servant region
BBODMNC	BBO8DMNC	Location service daemon

The cataloged-procedure names follow the same pattern as for the standalone application server. The D in the controller and servant procedure names indicates a deployment manager, and the C at the end of the location service daemon job name and cataloged-procedure name indicate an ND cell (as opposed to the B used for a base or standalone application server cell). The B and C in these names are values inherited from previous releases.

Default values for a managed node

When a managed (custom) node—an application server node with no servers that is intended for federation into a Network Deployment cell—is built, the name of the cell into which it will be federated is not actually specified. The managed node is created with a temporary cell name that must be different from the Network Deployment cell name. Therefore, the same defaults are used as those used for a standalone application server. Although this means that the configuration file system and mount point incorporate the temporary cell name, this can be corrected manually during customization if necessary.

The SAF groups, user IDs, and cataloged-procedure names are the same as those used for a standalone application server. However, an empty managed node does not have an application server; it only has a node agent (for node administration) until new servers are created in the node. The node agent has default server short name BBON001 and server long name nodeagent, which is fixed by the product architecture.

Default values for an administrative agent

An administrative agent controls one or more standalone application servers without requiring that they be federated into a Network Deployment cell.

By default, an administrative agent is built with cell short name BBOADMA, node short name BBOADMA, and server short name BBOADMA. The corresponding long names are cell name bboadma, node name bboadma, and server name admiagent, which is fixed by the product architecture. Like a deployment manager, the administrative agent can never be clustered; therefore, its default server generic short name, which is used to identify the administrative agent to Workload Management, is also set to BBOADMA.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS85.BBOADMA.BBOADMA.HFS  
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv8config/bboadma/bboadma
```

The SAF groups and user IDs created during customization have the same default names as those used for the standalone application server in order to make it possible to register the standalone application server with the administrative agent.

The following job names and cataloged-procedure names are used for the various regions:

Table 14. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOADMA	BBO8GCR	Controller
BBOADMAS	BBO8GSR	Servant region
BBODMNG	BBO8DMNG	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use G to indicate an administrative agent.

This makes the MVS start command for the administrative agent very simple:

```
START  
BBO8GCR, JOBNAME=BBOADMA, ENV=BBOADMA.BBOADMA.BBOADMA
```

Default values for a job manager

A job manager can control an administrative agent's registered application server nodes or a deployment manager and its managed and unmanaged nodes. In fact, it can manage several of each. On a system using the basic naming convention, you can register either the standalone application server (through its administrative agent) or a Network Deployment cell (through its deployment manager) with the job manager.

By default, a job manager is built with cell short name BBOJMGR, node short name BBOJMGR, and server short name BBOJMGR. The corresponding long names are cell name bbojmgr, node name bbojmgr, and server name jobmgr (which is fixed by the product architecture). Like a deployment manager, the administrative agent can never be clustered; therefore, its default server generic short name, which is used to identify the job manager to Workload Management, is also set to BBOJMGR.

The default dataset name for the configuration file system is the following:

OMVS.WAS85.BBOJMGR.BBOJMGR.HFS
(or .ZFS if a zFS file system is selected)

and it is mounted at the following location:

/wasv8config/bbojmgr/bbojmgr

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Table 15. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOJMGR	BBO8JCR	Controller
BBOJMGRS	BBO8JSR	Servant region
BBODMNJ	BBO8DMNJ	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use J to indicate a job manager.

Default values for a secure proxy server

A secure proxy server is intended to run in the "demilitarized" zone (DMZ), across a firewall from the WebSphere Application Server cells for which it serves as a front end. Unlike a regular proxy server, it cannot be clustered; but it can be registered with an administrative agent to provide some remote administration capabilities.

By default, a secure proxy server is built with cell short name BBOPROX, node short name BBOPROX, and server short name BBOPROX. The corresponding long names are cell name bboprox, node name bboprox, and server name proxy1. The default server generic short name, which is used to identify the server to Workload Management, is BBOPROX.

The default dataset name for the configuration file system is the following:

OMVS.WAS85.BBOPROX.BBOPROX.HFS
(or .ZFS if a zFS file system is selected)

and it is mounted at the following location:

/wasv8config/bboprox/bboprox

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Table 16. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOPROX	BBO8XCR	Controller
BBOPROXS	BBO8XSR	Servant region
BBODMNX	BBO8DMNX	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use X to indicate a secure proxy server.

Default values for a secure proxy administrative agent

A secure proxy server can be registered with an administrative agent to provide some remote administration capabilities.

By default, a secure proxy administrative agent is built with cell short name BBOPRXA, node short name BBOPRXA, and server short name BBOPRXA. The corresponding long names are cell name bboprxa, node name bboprxa, and server name adminagent. The default server generic short name, which is used to identify the administrative agent to Workload Management, is BBOPRXA.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS85.BBOPRXA.BBOPRXA.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv8config/bboprxa/bboprxa
```

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Table 17. Job names and cataloged-procedure names.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOPRXA	BBO8YCR	Controller
BBOPRXAS	BBO8YSR	Servant region
BBODMNY	BBO8DMNY	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use Y to indicate a secure proxy administrative agent.

As with the regular administrative agent, the MVS start command is very simple:

```
START
BBO8YCR,JOBNAME=BBOPRXA,ENV=BBOPRXA.BBOPRXA.BBOPRXA
```

Where to go next

The basic naming convention is adequate for an introduction to the WebSphere Application Server for z/OS product. However, most enterprises will want to create at least two application server nodes, whether for test and production or to allow for failover in a Network Deployment cell. For these configurations, you must use a more complex server naming convention.

The WebSphere Application Server for z/OS standard naming convention is a straightforward extension of the basic naming convention. The BB0 and WS prefixes are replaced with a two-character cell identifier; this allows for several concurrent cells or groups of cells with similar administrative needs that sharing a common set of server user IDs. Cluster identifiers and a system identifier, which are specified during customization, provide additional flexibility. Read “z/OS standard naming convention” for more information.

z/OS standard naming convention

In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the `zpm` command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Defaults are used that follow the standard naming convention if one- and two-character cell, cluster, and system identifier values are specified during customization.

The standard naming convention is suitable for both initial and production use, and it allows you to create groups of cells and servers with each group sharing a common set of user IDs and group names. A group of cells and servers is distinguished by sharing the same cell identifier.

How the standard naming convention differs from the basic naming convention

While the basic naming convention supports at most a single Network Deployment cell and a single application server node on a given z/OS system, the standard naming convention allows for the creation of up to 936 separate administrative groups, each corresponding to a single two-character cell identifier, on a single z/OS system. Each of these administrative groups can include the following:

- One Network Deployment cell
- Up to 36 application server nodes
- Administrative agents, job managers, and secure proxy servers

This administrative group is not actually a part of the WebSphere Application Server architecture; it simply represents the fact that on z/OS, a group of cells can use a common set of SAF groups and user IDs, which in turn simplifies the setup of connections between these cells. On the other hand, using different SAF groups and user IDs for separate cells provides for administrative and runtime separation so that the cells using different SAF identities can interact only in ways that you specify or not at all.

Selecting cell, system, and cluster identifiers

If you want to use the standard naming convention, specify a cell identifier, system identifier, and (in some cases) a cluster identifier when you configure a new WebSphere Application Server cell or node using the Profile Management Tool.

Cell identifier

This two-character, uppercase-alphanumeric value is used to construct the names of the SAF user IDs and groups that will be used for all cells and servers that share the same cell identifier. Together with the system identifier, it is used to build cell names, node names, and other values.

To simplify interaction between two cells, create them using the same cell identifier. To minimize or prevent interaction between two cells, create them using different cell identifiers.

Restrictions:

- Separate Network Deployment cells must have separate cell identifiers.
- Because there are 36 possible system identifiers (A-Z and 0-9), up to 36 of each of the other types of WebSphere Application Server cells (job manager, administrative agent, and secure proxy) can share the same cell identifier as long as a separate system identifier is chosen that distinguishes each cell from the others of the same type.
- If a standalone application server is to be federated into a Network Deployment cell, security setup is considerably simpler if the application server uses the same SAF user IDs and groups as the Network Deployment cell. If both are created using the standard naming convention, configure them using the same cell identifier.
- An administrative agent must run under the same SAF groups as the standalone application servers that it administers. Configure them with the same cell identifier.

System identifier

This one-character, uppercase-alphanumeric value is used to distinguish the application server nodes in a Network Deployment cell and the various types of other servers from each other. The name comes from the practice of creating a Network Deployment cell with one application server node on each z/OS system that the cell spans. However, the one-character identifier can also be used to distinguish several nodes on the same z/OS system or to identify several single-node cells that have the same cell identifier. In these latter cases, the system identifier does not have to represent an actual z/OS system.

For a Network Deployment cell with one node per z/OS system, assign a single alphanumeric character to each z/OS system and use that value when configuring the federated or managed application server nodes on that system. For other types of cells, you can assign any desired convention for the system identifier as long as no two servers of the same type share both a cell identifier and a system identifier.

Cluster identifier

This two-character, uppercase-alphanumeric value is used to distinguish application servers within an application server node. In order to allow for any application server to be used as the basis of an application server cluster, create each unclustered application server in a Network Deployment cell with its own cluster identifier. In the examples at the end of this article, the cluster identifier is given as a two-digit number to make it easy to identify the parts of each name.

Default values for cell, node, and server names

One Network Deployment cell and up to 36 of each of the other cell types can be configured with the standard naming convention under a single cell identifier by assigning a unique system identifier to each of the other cell types. In other words, two standalone application servers or two job managers that share a common cell identifier must have separate system identifiers.

Table 18. Default values for cell, node, and server names.

For cell identifier aa and system identifier s, the standard naming convention would assign the following cell and node names:

Name	ND Cell Deployment Manager	ND Cell Managed Node	Standalone Application Server	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Cell name	aaCELL	aaCELL	aaBASEs	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs
Node name	aaDMNODE	aaNODEs	aaNODEs	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs

Note that the Network Deployment cell has one deployment manager node and can have one application server node (managed or federated) for each system identifier. The node name for a standalone application server uses the same convention as the Network Deployment cell, allowing for easy federation.

The other server types use the same value as the cell name and node name because none of them require multiple nodes or an elaborate naming convention.

All of the names used so far are uppercase because they are z/OS short names, such as the cell short name and node short name, which must be uppercase. Each of these values also has a mixed-case long name, which is the internal WebSphere Application Server version of the name. For convenience, the standard naming convention uses the same value for the long name as for the short name but changes it to lowercase.

Server names are constructed from the cell identifier, system identifier, and (in the case of application servers) the cluster identifier. A Network Deployment cell can have only one deployment manager, and each of the other non-application server types has only a single server. Each server is also assigned a generic short name that is used to identify the server to Workload Management and is also used as the initial cluster name for application servers being clustered.

Table 19. Default values for server names and generic server short names.

For cell identifier aa, system identifier s, and cluster identifier nn, the standard naming convention would assign the following server names and generic server short names:

Name	ND Cell Deployment Manager	Application Server in an ND Cell or Standalone	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Server name	aaDMGR	aaSRnns	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs
Generic name	aaDMGR	aaSRnn	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs

This application server naming convention allows additional servers to be created in an application server node following the same naming convention, and it also makes clustering easier.

Defaults for SAF group and user ID names

Table 20. Default values for SAF group and user ID names.

For cell identifier cc, the following SAF groups and user IDs are created during customization:

ccCFG	Configuration group Provides administration and server privileges
ccSRVG	Servant group Provides privileges needed by servant regions
ccGUESTG	Unauthenticated, local user, or guest group Provides basic privileges to access the cell but nothing more
ccACRU	Controller user ID Controller, control region adjunct, and daemon started tasks
ccASRU	Servant user ID Servant started tasks
ccADMIN	Administrator user ID Used for cell configuration and, in certain circumstances, as a WAS administrator
ccGUEST	Unauthenticated-user user ID (z/OS-managed security only) Represents an unknown user for security purposes

Default values for configuration file system names and mount points

Each WebSphere Application Server cell or managed node has its own configuration file system, which might be either an HFS or zFS dataset. When cell, system, and cluster identifiers are specified during configuration, each configuration file system is assigned a unique dataset name:

`OMVS.MNT.cell_short_name/node_short_name.HFS`
(for an HFS dataset)

`OMVS.MNT.cell_short_name/node_short_name.ZFS`
(for a zFS dataset)

You can modify these names to fit local conventions, but make it clear which cell and node are associated with each dataset. The default mount points for these configuration file systems use the cell and node long names (simply lowercase versions of the long names by default) for readability:

`/wasv8config/cell_long_name/node_long_name`

The datasets can be renamed, but the mount points should not be changed after initial customization because they are referred to throughout the configuration files. One result of this is that when a standalone application server is federated into a Network Deployment cell, it retains its original configuration mount point even if that mount point contains the old (standalone) cell name. Users who know that a standalone application server is to be federated into a particular Network Deployment cell might want to manually update the configuration file system dataset name and mount point during creation of the standalone application server to reflect the node's eventual cell name.

Default values for job names and cataloged-procedure names

Most application servers consist of a controller (control region) and one or more servants (servant regions). An application server also has a messaging region called a control region adjunct. The job name for the control region is the same as the server short name. The initial job name for the servant consists of the server short name followed by an S, while the initial job name for the control region adjunct consists of the server short name followed by an A. (This is why server short names are customarily limited to a length of seven characters.)

Each control region, servant region, and control region adjunct requires a cataloged procedure that points to the server's configuration file system. In practice, this means that each node has its own controller, servant, and (in some cases) control region adjunct cataloged procedures; but the different servers in an application server node do not need their own cataloged procedures because they share a configuration file system.

Table 21. Default values for job names and cataloged-procedure names.

For cell identifier aa and system identifier s, the standard naming convention would assign the following job names and cataloged-procedures names. In each case, the controller job or procedure name is given first and followed by the job or procedure name for the servant and (if present) the control region adjunct:

Name	ND Cell Deployment Manager	Application Server Node (Node Agent in ND Cell)	Application Nerver Node (Application Server)	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Controller job name	ccDMGR	ccAGNTs	ccSRnns	ccADMAs	ccJMGRs	ccPROXs	ccPRXAs
Servant job name	ccDMGRs	ccAGNTsS	ccSRnnsS	ccADMAsS	ccJMGRsS		ccPRXAsS
Adjunct job name			ccSRnnsA				
Controller procedure	ccDCR	ccACRs	ccACRs	ccGCRs	ccJCRs	ccXCRs	ccYCRs
Servant procedure	ccDSR	ccASRs	ccASRs	ccGSRs	ccJSRs		ccYSRs
Adjunct procedure			ccAARs				

Table 22. Default values for location service daemon.

Each WebSphere Application Server cell also requires a location service daemon, which is used for all nodes of the cell on a given z/OS system:

Name	ND Cell (All Nodes)	Standalone Application Server	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Daemon job name	ccDEMNs	ccDEMNs	ccDMNGs	ccDMNJJs	ccDMNXs	ccDMNYs
Daemon procedure	ccDEMNs	ccDEMNs	ccDMNGs	ccDMNJJs	ccDMNXs	ccDMNYs

Configuration Planning Spreadsheets for z/OS

The configuration planning spreadsheets were developed to create response files that can then be imported into the Profile Management Tool.

Before you begin

A well-constructed WebSphere Application Server for z/OS cell will have a set of names and ports that are consistent and orderly. To assist in that process, Microsoft Excel spreadsheets have been developed that take a small set of key variables as input and produce a properly arranged set of names and ports and other values. Each spreadsheet creates a response file format ready for copy-and-paste into a file that can then be imported into the Profile Management Tool. Using both a spreadsheet and the Profile Management Tool greatly simplifies the process of creating a configuration and it enforces a number of naming best practices. The spreadsheets have proven to be effective and timesaving tools for administrators of WebSphere Application Server for z/OS.

Procedure

Go to the Techdocs - the Technical Sales Library, search for WebSphere for z/OS Version 8.5 - Configuration Planning, click the link to the Version 8.5 spreadsheets, and download the spreadsheets that you need.

Default port assignments

This article lists the default server values for WebSphere Application Server for z/OS.

WebSphere Application Server for z/OS port assignments

Table 23. Default port assignments.

This table lists the default port values for WebSphere Application Server for z/OS.

Port Name	Default Value					
	Standalone Application Server	Deployment Manager	ND Node Agent	ND Managed Node	Administrative Agent	Job Manager
HTTP Transport Port (WC_defaulthost)	9080			9080		
HTTPS Transport Secure Port (WC_defaulthost_secure)	9443			9443		
Administrative Console Port (WC_adminhost)		9060		9060	9060	9960
Administrative Console Secure Port (WC_adminhost_secure)		9043		9043	9043	9943
Administrative Interprocess Communication Connector Port (IPC_CONNECTOR_ADDRESS)	9633	9632			9630	9631

Table 23. Default port assignments (continued).

This table lists the default port values for WebSphere Application Server for z/OS.

Port Name	Default Value					
	Standalone Application Server	Deployment Manager	ND Node Agent	ND Managed Node	Administrative Agent	Job Manager
Bootstrap Port (BOOTSTRAP_ADDRESS)	2809	9809	2809	9810		
ORB	2809	9809	2809	9810	9807	9808
ORB SSL	0	0	0	0	0	0
SOAP/JMX (SOAP_CONNECTOR_ADDRESS)	8880	8879	9360	8880	8877	8876
Node Discovery Address (NODE_DISCOVERY_ADDRESS)			7272			
Node Multicast Discovery Address (NODE_MULTICAST_DISCOVERY_ADDRESS)			5000			
Cell Discovery Address (CELL_DISCOVERY_ADDRESS)		7277				
Service Integration Port (SIB_ENDPOINT_ADDRESS)	7276					
Service Integration Secure Port (SIB_ENDPOINT_SECURE_ADDRESS)	7286					
Service Integration MQ Interoperability Port (SIB_MQ_ENDPOINT_ADDRESS)	5558					
Service Integration MQ Interoperability Secure Port (SIB_MQ_ENDPOINT_SECURE_ADDRESS)	5578					
Session Initiation Protocol Port (SIP_DEFAULTHOST)	5060					
Session Initiation Protocol Secure Port (SIP_DEFAULTHOST_SECURE)	5061					
High Availability Manager Communications (DCS_UNICAST_ADDRESS)	9353	9352	9354			
DataPower Application Manager		5555				
Daemon Port	5655	5755				
Daemon SSL Port	5656	5756				

Location service daemon ports

Standalone application server node location service daemons are considered temporary. The ports assigned to a standalone application server node's location service daemon are used only until that node is federated. It is advisable to set aside a couple of ports to serve as interim ports for the standalone application server node location service daemon. The permanent location service daemon ports are the ones assigned to the deployment manager. Those same ports are copied to location service daemons created when a standalone application server node on another MVS image is federated into the deployment manager cell.

Node agent ports

There is a node agent per MVS image on which the cell spans. One design option calls for all node agents to have the exact same ports so the Sysplex Distributor is able to balance the traffic between the two. The node agent is created when the BBOWADDN customized job is run.

Server clusters

A server cluster is a grouping of two or more servers into a one logical server. A cluster is created through the administrative console. Servers within a cluster are called cluster members. Servers (members) within a cluster start out being clones of one another. When it comes to the TCP ports for the members in a cluster, the administrative console allows you during the creation of the cluster to specify if you want the HTTP ports to be unique or the same. The other ports -- bootstrap, DRS, ORB, ORB SSL and SOAP -- will be made unique by the application server.

For complex configurations with multiple members in a cluster it is advisable to make the members be as nearly identical to one another as possible, including the TCP ports. Therefore, when planning it is recommended a range of ports be allocated for a cluster with the intention to make certain all members of that cluster were given the same set of ports. Because WebSphere will automatically generate unique DRS, ORB, ORB SSL and SOAP ports for the second cluster member, it is necessary to go back in and remap the ports back to the ports set aside for the server cluster

Note: When a vertical cluster, two members on the same MVS image, is the potential configuration, you will need to consider port sharing by two members of the same cluster on the same MVS image.

Initial security configurations

During installation you now have the option of enabling administrative security during initial cell customization, this procedure is referred to as "security out of the box". This protects the cell from unauthorized modification, which can occur if security is not enabled.

When a new standalone application server or Network Deployment cell is created, there are three initial security choices in WebSphere Application Server for z/OS Version 8.5:

- Use a z/OS security product to manage user identities and authorization policy
- Use WebSphere Application Server to manage user identities and the authorization policy
- Do not enable security

This article describes the three initial security options and the configuration effects of each.

Remember that WebSphere Application Server for z/OS always requires the presence of a SAF-compliant security system to provide operating system security. Regardless of which security option is chosen:

- SAF user IDs for WebSphere Application Server started tasks are always created during customization.
- SAF groups are created for the configuration, servant and local user groups are created during customization, and granted necessary permissions
- SAF SERVER profiles are used to control servant access to controller regions.
- If daemon SSL is selected during customization, a key ring and digital certificate for the daemon are created in SAF.

Note: Each of the initial security configurations is basic, requiring few choices during customization; after configuration is complete, additional work is usually required to match cell security policies to the needs of the enterprise. See the Security section of the InfoCenter for more information.

Option 1: Use a z/OS security product to manage user identities and authorization policy

If this option is chosen during customization:

1. Each WebSphere Application Server user and group identity corresponds to a user ID or group in the z/OS system's SAF-compliant security system (IBM'S RACF, or an equivalent product).
2. Access to WebSphere Application Server roles is controlled using the SAF EJBROLE profile.
3. Digital certificates for SSL communication are stored in the z/OS security product.

The z/OS system's security product is always used to control WebSphere Application Server for z/OS started task identities, and the location service daemon's digital certificate (if daemon SSL is selected). However, when this security option is selected, all WebSphere Application Server administrators and administrative groups must be defined to SAF as well. Later, if application security is enabled, the SAF security database holds those user identities as well.

This option is appropriate when servers or cells will reside entirely on z/OS systems, with SAF as the user registry. Customers who plan to implement an LDAP or custom user registry, but who will map WebSphere Application Server identities to SAF identities and use EJBROLE profiles for authorization, should also choose this option so that initial SAF EJBROLE setup is performed.

When this option is chosen during customization, the following SAF user IDs are created:

- An administrator user ID
- An unauthorized-user ID, to represent WebSphere Application Server identities which have not been authenticated

SAF EJBROLE profiles for administrative roles (administrator, configuration, deployer, monitor and operator) are created, and the administrator user ID is granted the administrator role.

SAF CBIND profiles are created, and granted to the configuration group.

Digital certificates are created in the SAF security system for each server controller (deployment manager or application server controller).

Digital key rings are created in the SAF security system for the administrator, controller, controller region adjunct, and server user IDs, and the appropriate certificates are attached to these key rings.

A SAF profile prefix may be specified when this option is chosen; the SAF profile prefix becomes part of the APPL, CBIND and EJBROLE profile names used for authorization checking.

Option 2: Use WebSphere Application Server to manage user identities and authorization policy

If this option is chosen during customization:

1. Each WebSphere Application Server user and group identity corresponds to an entry in a WebSphere Application Server user registry. The initial user registry is a simply file-based user registry, created during customization, and residing in the configuration file system.
2. Access to WebSphere Application Server roles is controlled using WebSphere Application Server role bindings. In particular, administrative roles are controlled using the console users and groups settings in the administrative console.
3. Digital certificates for SSL communication are stored in the configuration file system.

The z/OS system's security product is always used to control WebSphere Application Server for z/OS started task identities, and the location service daemon's digital certificate (if daemon SSL is selected). However, when this security option is selected, all WebSphere Application Server users and groups for

administrative access are defined in the WebSphere user registry, rather than in SAF. Later, if application security is enabled, the WebSphere Application Server user registry holds those user identities as well.

This option is appropriate when servers or cells will reside on a mix of z/OS and non-z/OS systems, as well as for customers who plan to implement an LDAP or custom user registry to replace the initial registry. (Customers who plan to implement an LDAP or custom user registry with identity mapping to SAF should select z/OS-managed security during customization; see above.)

When this option is chosen during customization, a file-based user registry is created in the configuration file system.

An administrator user ID is added to the file-based user registry.

The administrator user ID is added to the list of authorized console users.

Self-signed digital certificates for servers are created in the configuration file system automatically by WebSphere Application Server.

Option 3: Do not enable security

If this option is chosen, no administrative security is configured. Anyone with access to the administrative console port can make changes to the server or cell configuration.

A post-customization security setup is recommended.

The initial security setup options in WebSphere Application Server are very basic, and are intended only to provide initial administrative security. After your server or cell is up and running, you may wish to:

- Switch to another user registry. You can use LDAP or a custom user registry instead of the SAF security database or file-based registry.
- Define additional administrators, or distribute administrative roles
- Implement application security

Building practice WebSphere Application Server for z/OS cells

Use this task to practice configuring WebSphere Application Server for z/OS. If you are installing the product for the first time without migration from an earlier version, it is helpful to install a practice application serving environment in order to learn the customization process.

Before you begin

Note the following when you install your practice runtime:

- Be careful when typing and following the instructions in the customization.
- Note the user ID requirements in the generated instructions. If your user IDs are not configured correctly, the jobs might not run successfully.
- Keep track of each step so that you do not skip or repeat any steps.
- Examine each job's output (not only the return code) to confirm that everything is configured correctly. Sometimes, the return code indicates no problems but the job output contains errors. For a proper configuration, you should have no errors in your job output unless the instructions specifically describe errors in the job output.

About this task

You should install a practice runtime when you install WebSphere Application Server on z/OS for the first time and want to learn the steps for installing and customizing it.

Install using either the Profile Management Tool or the `zpm` command.

Procedure

1. Print a copy of the “z/OS customization worksheet: Standalone application servers for Version 7.0” on page 133 and fill it out using “z/OS customization variables: Standalone application servers” on page 118 as a guide.

Note: Make sure that the user ID names, group names, UID/GID values, and TCP/IP port numbers that you specify are not already being used on your z/OS system.

2. Read the “Using the Profile Management Tool (z/OS only)” on page 429 article.
3. Follow the steps in “Creating standalone application server cells on z/OS using the Profile Management Tool” on page 436. View and follow the generated instructions, which tell you how to:
 - Perform the manual configuration updates in the generated standalone application server instructions. These steps affect parts of your system that are usually controlled. These are changes that the systems programmer responsible for your z/OS system should review.
 - Update your server-specific security definitions.

The next job (BBOCBRAK) issues the RACF commands necessary for defining the users, groups, profiles, and permissions for the WebSphere Application Server for z/OS runtime servers. Submit the BBOCBRAK job, or take it to your security administrator for approval. Your security administrator should issue those commands or submit the supplied jobstreams. If your installation has a different profile structure, you might have to modify the RACF commands generated by this exec to suit your particular needs.

Note: Your installation must have "list of groups" on for these commands to work because the servers must be connected to the WebSphere Application Server for z/OS administrator group.

- Create the configuration file system and WebSphere Application Server for z/OS home directory for your server. Jobs BBOWCFS and BBOWHFS (run at this point) and job BBOWWPFA (see below) run BPXBATCH shell scripts to define, customize, and load data into the configuration HFS and manipulate the ownership and permission attributes. For this reason, you must run these jobs under a user ID with UID=0.
- Create cataloged procedures for the server.
- Set up the runtime (configuration) file system for the new application server. The BBOWWPFA job might run for some time. The BBOWHFSB job cleans up the configuration file system and makes sure that all file ownerships are correct.
- Start the new standalone application server, and run the Install Verification Test (IVT).

Notes:

- If the BBOWWPFA (profile creation) job fails with the following error:

```
Cannot use the directory: The /WebSphere/V8R5M0/AppServer/profiles/default
directory exists and is not empty.
INSTCONFFAILED: Cannot create profile: The profile does not exist.
```

delete the `was_home/profiles/default` directory and all its contents before rerunning BBOWWPFA.

- If you have some other security product such as Top Secret or ACF2 instead of RACF, contact your security system vendor for the appropriate security system commands needed to configure WebSphere Application Server for z/OS. You might need to contact the vendor for the latest maintenance and guidance on WebSphere Application Server for z/OS customization.

4. Troubleshoot any problems you encounter while customizing your application server.

If you encounter problems while customizing your application server, review the steps that you have performed--especially regarding such things as specific user IDs under which jobs must be run. Check all job output for any error messages that you might have missed.

Watch out for these common mistakes:

- Navigating the configuration file system with a UID of 0 can alter files or their ownership and permission attributes, making them inaccessible to the WebSphere Application Server for z/OS runtime servers and administrators. To avoid this problem, use the WebSphere Application Server for z/OS administrator user ID.
- If you decide to change any of the customized variables after you submit any of these jobs, do not make manual modifications to the generated jobstreams or data. Cancel the installation, and start over by regenerating all the jobstreams and start over from the BBOWHFS job.

Results

After you have successfully followed the instructions, you will have set up a WebSphere Application Server for z/OS standalone application server.

What to do next

Read the concept articles under Chapter 8, “Planning for product configuration on z/OS,” on page 77 and plan one or more application serving environments that fit your system environment and business needs.

You might want to delete the practice application server that you just set up in order to save space on your system, to clean up your datasets, or for other reasons. Follow these steps to delete it from your system:

1. Stop the server.
2. Unmount and delete the configuration file system.
3. Delete the cataloged procedures.
4. Remove any TCP/IP port reservations for the practice application server.
5. Delete the RACF user IDs, groups, and profiles that you have created unless you use the same users and groups for a different WebSphere Application Server for z/OS cell.

Planning for standalone application server cells

About this task

A standalone application server cell is the simplest WebSphere Application Server for z/OS configuration on which you can deploy and run applications. A standalone application server cell includes the following:

- Basic cell and node configuration
- Location service daemon
- Application server that runs the administrative console application

You can deploy and run additional applications on this server.

Although you can define additional application servers in the standalone cell, you cannot manage them using the standalone server version of the administrative console. If you wish to define and manage multiple application servers in a standalone application server node, you can either define an administrative agent and register the standalone appserver server node with it or define a Network Deployment cell and federate the application server node into the Network Deployment cell. The administrative agent or the Network Deployment cell's deployment manager can then be used to manage the application servers in the standalone application server node.

If you have never configured a WebSphere Application Server for z/OS cell, try “Building practice WebSphere Application Server for z/OS cells” on page 115 first.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Standalone application servers.”
3. Save the worksheet for use during standalone application server customization.

z/OS customization variables: Standalone application servers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a standalone application server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server runtime performance tuning setting

Performance-tuning setting that most closely matches the type of environment in which the application server will run

Standard

The standard settings are optimized for general-purpose usage.

Peak The peak-performance settings are appropriate for a production environment where application changes are rare and optimal runtime performance is important.

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell, cluster, and system identifiers

When this option is selected, default cell, node, server, cluster, and procedure names as well as group names and user IDs are based on cell, cluster, and system identifiers.

Application server will be federated into a Network Deployment cell

Select this option to indicate that the application server will be federated into a Network Deployment cell. In this case, specify the two-character cell identifier of the target Network Deployment cell.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Two-character cluster identifier

Two-character cluster identifier to be used to create default names and user IDs

Rule: The characters must be alphabetic characters. The alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 20 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is

safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs (provides minimal access to the cell)

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users**Common controller user ID****User ID**

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID**User ID**

User ID associated with the servant and control adjunct regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator

User ID

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Configure Additional Users

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Controller adjunct user ID

User ID

User ID associated with the control adjunct

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control adjunct user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Daemon user ID

User ID

User ID associated with the daemon

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the daemon user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMB0LS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMB0LS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a Network Deployment cell, ensure that the standalone server cell name is different from the Network Deployment cell name.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names

Short name

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Server names

Short name

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server job name.

Rules: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name

WLM APPLENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. You might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System**Product file system directory**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream**Error log stream name (optional)**

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.

- Do not put quotes around the name.

CTRACE parmlib member

CTRACE parmlib member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Optional Application Deployment

Deploy the administrative console

Specify whether to install a Web-based administrative console that manages the application server.

Deploying the administrative console is recommended, but if you deselect this option, the information center contains detailed steps for deploying it after the profile exists.

Deploy the default application

Specify whether to install the default application that contains the Snoop, Hello, and HitCount servlets.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Controller adjunct process

Job name

Job name used by WLM to start the control region adjunct

This is set to the server short name followed by the letter A, and it cannot be changed through the tool.

Procedure name

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must be seven or fewer characters.

Servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the `virtualhosts.xml` file, which makes setting a specific IP address here less than ideal. If you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port

Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port

Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

HTTP transport port

Port for HTTP requests (WC_defaulthost)

Rule: Value cannot be 0.

HTTPS transport port

Port for secure HTTP requests (WC_defaulthost_secure)

Rule: Value cannot be 0.

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

Service integration port

Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration secure port

Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability port

Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability secure port

Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Session initiation protocol (SIP) port

Port for session initiation requests (SIP_DEFAULTHOST)

Rule: Value cannot be 0.

Session initiation protocol (SIP) secure port

Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Rule: Value cannot be 0.

Administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_UDP_LISTENER_ADDRESS)

Administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_TCP_LISTENER_ADDRESS)

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for enterprise beans for example) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization

Note: If you plan to federate this application server into a Network Deployment cell, you might want to set the application server's SAF key ring name to be the same as that of the Network Deployment cell.

Certificate authority keylabel

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection**Use a z/OS security product**

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

Note: If you plan to federate this application server into a Network Deployment cell, you might want to set the application server's SAF profile prefix to be the same as that of the Network Deployment cell.

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Web Server Definition

Notes:

- You will not be able to administer a web server through the integrated solutions console on a standalone application server until it is federated.
- You can only have one web server defined on a standalone application server.

Create a web server definition

Indicates whether to create a web server definition.

You can only have one web server defined on a standalone application server.

Web server type

Select the web server type from the list of supported web servers.

Web server operating system

Operating system where the web server is located

Web server name

Name used in defining the web server to WebSphere Application Server

Web server host name or IP address

IP name or address of the system on which the web server is located

Web server port

HTTP port on which the web server listens

Web server installation directory path

Name of the directory where the web server is installed

Web server plug-in installation directory path

Name of the directory where the web server plug-ins are installed

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Standalone application servers for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this standalone application server:

System name: _____

Sysplex name: _____

Table 24. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAppSrvxx	
Response file path name (optional)	None	
Server runtime performance tuning setting (standard or peak) *	Standard	

* Do not use the peak setting unless the target WebSphere Application Server for z/OS node is at Version 7.0.0.15 or later.

Table 25. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		

Table 25. Default Values (continued).

Enter your values:

Item		Default	Your value
	Application server will be federated into a Network Deployment cell	Not selected	
	Set default names and userids based on cell, system, and cluster identifiers	Not selected	
	Two-character cell identifier	AZ	
	Two-character cluster identifier	00	
	Single-character system identifier	A	
Port defaults			
	Set default port values from the following port range	Not selected	
	Lowest default port number	9530	
	Highest default port number	9549	

Table 26. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 27. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			

Table 27. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 28. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2431	
Common servant user ID			
	User ID	WSSRU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2432	
WebSphere Application Server administrator			
	User ID	WSADMIN	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2403	
Asynchronous administration user ID			
	User ID	WSADMSH	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2504	
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 29. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Controller adjunct user ID			

Table 29. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
	User ID	WSCRAU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2433
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 30. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 31. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOBASE	
	Long name	bbobase	
Node names			
	Short name	BBONODE	
	Long name	bbonode	
Server names			
	Short name	BBOS001	
	Long name	server1	
Cluster transition name		BBOC001	
JVM mode			
	31 bit	Not selected	
	64 bit	Selected	

Table 32. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
	Hierarchical File System (HFS)	Selected
	zSeries File System (ZFS)	Not selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 33. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe

Table 34. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOBASE.ERROR. LOG
CTRACE parmlib member		

Table 34. Error Log Stream and CTRACE Parmlib Member (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
CTRACE parmlib member suffix (optional)	60	

Table 35. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	
Deploy the default application	Selected	
Deploy the sample applications	Not selected	

Table 36. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
Job name	<i>server_short_name</i>	<i>server_short_name</i>
Procedure name	BBO7ACR	
Controller adjunct process		
Job name	<i>server_short_nameA</i>	<i>server_short_nameA</i>
Procedure name	BBO7CRA	
Servant process		
Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
Procedure name	BBO7ASR	
Admin asynch operations procedure name	BBO7ADM	

Table 37. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
JMX SOAP connector port	8880	
ORB listener IP address	*	
ORB listener port	2809	
ORB SSL listener port	0	

Table 37. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value	
HTTP transport IP address	*		
	Administrative console port	9060	
	Administrative console secure port	9043	
	HTTP transport port	9080	
	HTTPS transport port	9443	
Administrative interprocess communication port (K)	9633		
High Availability Manager communication port (DCS)	9353		
Service integration port	7276		
Service integration secure port	7286		
Service integration MQ interoperability port	5558		
Service integration MQ interoperability secure port	5578		
Session initiation protocol (SIP) port	5060		
Session initiation protocol (SIP) secure port	5061		

Table 38. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv7config/ cell_long_name/ node_long_name/Daemon	/wasv7config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNB	
Procedure name	BBO7DMNB	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 39. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	

Table 39. SSL Customization (continued).

Enter your values:

Item	Default	Your value
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Enable SSL on location service daemon	Selected	

Table 40. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 41. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 42. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	
Sample applications		
User name	samples	samples
Password	None	

Table 43. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 44. Web Server Definition (Part 1).

Enter your values:

Item	Default	Your value
Create a web server definition		Not selected
	Web server type	IBM HTTP Server
	Web server operating system	z/OS
	Web server name	webserver1
	Web server host name or IP address	host_name
	Web server port	80

Table 45. Web Server Definition (Part 2).

Enter your values:

Item	Default	Your value
Web server installation directory path	/etc/websrv1	
Web server plug-in installation directory path	/etc/websrv1/Plugins	

Table 46. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	

Table 46. Job Statement Definition (continued).

Enter your values:

Item	Default	Your value
//*	//*	
//*	//*	

z/OS customization worksheet: Standalone application servers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this standalone application server:

System name: _____

Sysplex name: _____

Table 47. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAppSrvxx	
Response file path name (optional)	None	
Server runtime performance tuning setting (standard or peak)	Standard	

Table 48. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		

Table 48. Default Values (continued).

Enter your values:

Item		Default	Your value
	Application server will be federated into a Network Deployment cell	Not selected	
	Set default names and userids based on cell, system, and cluster identifiers	Not selected	
	Two-character cell identifier	AZ	
	Two-character cluster identifier	00	
	Single-character system identifier	A	
Port defaults			
	Set default port values from the following port range	Not selected	
	Lowest default port number	9530	
	Highest default port number	9549	

Table 49. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 50. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			

Table 50. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 51. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRUI	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2431	
Common servant user ID			
	User ID	WSSRU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2432	
WebSphere Application Server administrator			
	User ID	WSADMIN	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2403	
Asynchronous administration user ID			
	User ID	WSADMSH	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2504	
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 52. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
Controller adjunct user ID		

Table 52. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
	User ID	WSCRAU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2433
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 53. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 54. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOBASE	
	Long name	bbobase	
Node names			
	Short name	BBONODE	
	Long name	bbonode	
Server names			
	Short name	BBOS001	
	Long name	server1	
Cluster transition name		BBOC001	

Table 55. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 56. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall

Table 57. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOBASE.ERROR. LOG
CTRACE parmli member		

Table 57. Error Log Stream and CTRACE Parmlib Member (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmliib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
CTTRACE parmliib member suffix (optional)	60	

Table 58. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	
Deploy the default application	Selected	

Table 59. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
Job name	<i>server_short_name</i>	<i>server_short_name</i>
Procedure name	BBO8ACR	
Controller adjunct process		
Job name	<i>server_short_nameA</i>	<i>server_short_nameA</i>
Procedure name	BBO8CRA	
Servant process		
Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
Procedure name	BBO8ASR	
Admin asynch operations procedure name	BBO8ADM	

Table 60. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
JMX SOAP connector port	8880	
ORB listener IP address	*	
ORB listener port	2809	
ORB SSL listener port	0	
HTTP transport IP address	*	

Table 60. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Administrative console port	9060	
Administrative console secure port	9043	
HTTP transport port	9080	
HTTPS transport port	9443	
Administrative interprocess communication port	9633	
High Availability Manager communication port (DCS)	9353	
Service integration port	7276	
Service integration secure port	7286	
Service integration MQ interoperability port	5558	
Service integration MQ interoperability secure port	5578	
Session initiation protocol (SIP) port	5060	
Session initiation protocol (SIP) secure port	5061	

Table 61. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv8config/ cell_long_name/ node_long_name/Daemon	/wasv8config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNB	
Procedure name	BBO8DMNB	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 62. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	

Table 62. SSL Customization (continued).

Enter your values:

Item	Default	Your value
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 63. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 64. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 65. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 66. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		

Table 66. Security Certificate (continued).

Enter your values:

Item		Default	Your value
	Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
	Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
	Expiration period in years	1	
Root signing certificate			
	Expiration period in years	25	
Default keystore password			

Table 67. Web Server Definition (Part 1).

Enter your values:

Item		Default	Your value
Create a web server definition		Not selected	
	Web server type	IBM HTTP Server	
	Web server operating system	z/OS	
	Web server name	webserver1	
	Web server host name or IP address	<i>host_name</i>	
	Web server port	80	

Table 68. Web Server Definition (Part 2).

Enter your values:

Item		Default	Your value
Web server installation directory path		/etc/websrv1	
Web server plug-in installation directory path		/etc/websrv1/Plugins	

Table 69. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	

Table 69. Job Statement Definition (continued).

Enter your values:

Item	Default	Your value
//*	//*	

z/OS customization worksheet: Standalone application servers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this standalone application server:

System name: _____

Sysplex name: _____

Table 70. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAppSrvxx	
Response file path name (optional)	None	
Server runtime performance tuning setting (standard or peak)	Standard	

Table 71. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		

Table 71. Default Values (continued).

Enter your values:

Item		Default	Your value
	Application server will be federated into a Network Deployment cell	Not selected	
	Set default names and userids based on cell, system, and cluster identifiers	Not selected	
	Two-character cell identifier	AZ	
	Two-character cluster identifier	00	
	Single-character system identifier	A	
Port defaults			
	Set default port values from the following port range	Not selected	
	Lowest default port number	9530	
	Highest default port number	9549	

Table 72. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 73. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			

Table 73. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 74. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2431	
Common servant user ID			
	User ID	WSSRU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2432	
WebSphere Application Server administrator			
	User ID	WSADMIN	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2403	
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 75. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Controller adjunct user ID			
	User ID	WSCRAU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2433	
Daemon user ID			

Table 75. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
User ID	WSDMNU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2434	

Table 76. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 77. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOBASE	
Long name	bbobase	
Node names		
Short name	BBONODE	
Long name	bbonode	
Server names		
Short name	BBOS001	
Long name	server1	
Cluster transition name	BBOC001	

Table 78. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	

Table 78. Configuration File System (continued).

Enter your values:

Item		Default	Your value
File system type			
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.			

Table 79. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 80. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOBASE.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 81. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	
Deploy the default application	Selected	

Table 82. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8ACR
Controller adjunct process		
	Job name	<i>server_short_nameA</i>
	Procedure name	BBO8CRA
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8ASR

Table 83. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		None
	JMX SOAP connector port	8880
ORB listener IP address		*
	ORB listener port	2809
	ORB SSL listener port	0
HTTP transport IP address		*
	Administrative console port	9060
	Administrative console secure port	9043
	HTTP transport port	9080
	HTTPS transport port	9443
Administrative interprocess communication port		9633
High availability manager communication port (DCS)		9353
Service integration port		7276
Service integration secure port		7286

Table 83. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Service integration MQ interoperability port	5558	
Service integration MQ interoperability secure port	5578	
Session initiation protocol (SIP) port	5060	
SIP secure port	5061	
Administration overlay UDP port	11003	
Administration overlay TCP port	11004	

Table 84. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv85config/ cell_long_name/ node_long_name/Daemon	/wasv85config/cell_long_name/ node_long_name/ Daemon
Daemon job name	BBODMNB	
Procedure name	BBO8DMNB	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 85. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 86. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 87. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 88. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 89. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 90. Web Server Definition (Part 1).

Enter your values:

Item	Default	Your value
Create a web server definition	Not selected	
Web server type	IBM HTTP Server	
Web server operating system	z/OS	
Web server name	webserver1	
Web server host name or IP address	<i>host_name</i>	
Web server port	80	

Table 91. Web Server Definition (Part 2).

Enter your values:

Item	Default	Your value
Web server installation directory path	/etc/websrv1	
Web server plug-in installation directory path	/etc/websrv1/Plugins	

Table 92. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for administrative agents

An administrative agent provides a single interface to administer multiple standalone application servers.

Before you begin

Make sure that the nodes that you want the administrative agent to manage have the same products as the administrative agent, and the products are at the same version levels on these node and the administrative agent. This requirement is enforced because the administrative agent must have a matching environment in order to handle all of the administrative capabilities of the registered node. A node is not allowed to register with an administrative agent unless that node has an identical set of products and versions.

Note: If you were previously running on Version 7.0.0.11 or earlier and have an administrative agent with a managed node that has mismatched products or versions, when you migrate to Version 8.5, that administrative agent will not be able to start the subsystem for any mismatched nodes. You must

update these nodes to have the same products and versions as the administrative agents, restart the servers on the node and then restart the administrative agent, before the administrative agent can resume managing these registered nodes

About this task

An administrative agent can monitor and control multiple application servers on one or more nodes. By using a single interface to administer your application servers, you reduce the overhead of running administrative services in every application server.

Use the WebSphere Customization Toolbox or the `zpm` command and the customization jobs that they generate to configure an administrative agent on z/OS. The administrative agent must run on the same z/OS system as the application server nodes that it manages, and it must use the same SAF configuration group as the nodes to be managed.

After the administrative agent is up and running, you can use the following commands to register and unregister a node with the administrative agent:

- **registerNode**

Run the `registerNode` command to register a node with the administrative agent. When you run the command, the standalone node is converted into a node that the administrative agent manages. The administrative agent and the node being registered must be on the same system. You can only run the command on an unfederated node. If the command is run on a federated node, the command exits with an error.

Any node registered with the administrative agent automatically becomes eligible to register with the job manager.

- **deregisterNode**

Use the `deregisterNode` command to deregister a node from an administrative agent so that you can use the node standalone or register the node with another administrative agent. The node must have been previously registered with the administrative agent. When you deregister a node, the node configuration is retained but is marked as not registered with the administrative agent.

An administrative agent can register any of the profiles that it manages with a job manager.

For more information, read the *Administering nodes using the administrative agent* article in the information center.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Administrative agents.”
3. Save the worksheet for use during administrative agent customization.

z/OS customization variables: Administrative agents

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure an administrative agent.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type

Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell and system identifiers

When this option is selected, default cell, node, server, and procedure names as well as group names and user IDs are based on a cell and system identifiers.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID**User ID**

User ID associated with the servant region

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator**User ID**

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Configure Additional Users

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Daemon user ID

User ID

User ID associated with the daemon

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the daemon user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMBOLS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMBOLS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Note: Each management server (administrative agent, deployment manager, or job manager) should be assigned its own cell name that is different from that of any other WebSphere Application Server cell on the same z/OS sysplex.

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names

Short name

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names

Short name

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Cluster transition name

WLM APPLENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System**Product file system directory**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream**Error log stream name (optional)**

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.

- Do not put quotes around the name.

CTRACE parmlib member

CTRACE parmlib member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the `virtualhosts.xml` file, which makes setting a specific IP address here less than ideal. If you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port

Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port

Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOp IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

The port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization

Certificate authority keylabel

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol

(IIOp) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate**Default personal certificate****Issued to distinguished name**

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Administrative agents for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 93. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 94. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Administrative agent

Table 95. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected

Table 95. Default Values (continued).

Enter your values:

Item		Default	Your value
Name and userid defaults			
	Set default names and userids based on cell and system identifiers	Not selected	
	Two-character cell identifier	AZ	
	Single-character system identifier	A	
Port defaults			
	Set default port values from the following port range	Not selected	
	Lowest default port number	9510	
	Highest default port number	9519	

Table 96. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 97. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 98. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		
User ID	WSADMIN	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2403	
WebSphere Application Server user ID home directory	/var/ WebSphere/ home	

Table 99. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
Daemon user ID		
User ID	WSDMNU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2434	

Table 100. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 101. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOADMA	
Long name	bboadma	
Node names		
Short name	BBOADMA	
Long name	bboadma	
Server names		
Short name	BBOADMA	
Long name	adminagent	adminagent
Cluster transition name	BBOADMA	

Table 102. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AdminAgent	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
Hierarchical File System (HFS)	Selected	
zSeries File System (ZFS)	Not selected	
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 103. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link		

Table 103. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe	

Table 104. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOADMA.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 105. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO7GCR	
Servant process			
	Job name	server_short_nameS	server_short_nameS
	Procedure name	BBO7GSR	

Table 106. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	JMX SOAP connector port	8877	
ORB listener IP address		*	
	ORB listener port	9807	
	ORB SSL port	0	
HTTP transport IP address		*	

Table 106. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port (K)	9630	

Table 107. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv7config/ cell_long_name/ node_long_name/Daemon	/wasv7config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNG	
Procedure name	BBO7DMNG	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 108. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Enable SSL on location service daemon	Selected	

Table 109. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 110. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 111. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 112. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 113. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	

Table 113. Job Statement Definition (continued).

Enter your values:

Item	Default	Your value
//*	//*	
//*	//*	

z/OS customization worksheet: Administrative agents for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 114. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 115. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Administrative agent

Table 116. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A

Table 116. Default Values (continued).

Enter your values:

Item	Default	Your value
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9510
	Highest default port number	9519

Table 117. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 118. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
	Group	WSCFG1
	Allow OS security to assign GID	Not selected
	Assign user-specified GID	Selected
	Specified GID	2500
WebSphere Application Server servant group information		
	Group	WSSR1
	Allow OS security to assign GID	Not selected
	Assign user-specified GID	Selected
	Specified GID	2501
WebSphere Application Server local user group information		
	Group	WSCLGP
	Allow OS security to assign GID	Not selected
	Assign user-specified GID	Selected
	Specified GID	2502

Table 119. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		

Table 119. Configure Common Users (continued).

Enter your values:

Item		Default	Your value
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 120. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 121. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 122. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOADMA	
Long name	bboadma	
Node names		
Short name	BBOADMA	
Long name	bboadma	
Server names		
Short name	BBOADMA	
Long name	adminagent	adminagent
Cluster transition name	BBOADMA	

Table 123. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AdminAgent	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
Hierarchical File System (HFS)	Not selected	
zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 124. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		

Table 124. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall	

Table 125. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOADMA.ERROR.LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 126. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO8GCR	
Servant process			
	Job name	server_short_nameS	server_short_nameS
	Procedure name	BBO8GSR	

Table 127. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	JMX SOAP connector port	8877	
ORB listener IP address		*	
	ORB listener port	9807	
	ORB SSL listener port	0	
HTTP transport IP address		*	

Table 127. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port	9630	

Table 128. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv8config/ cell_long_name/ node_long_name/Daemon	/wasv8config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNG	
Procedure name	BBO8DMNG	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 129. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 130. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	

Table 130. Administrative Security Selection (continued).

Enter your values:

Item	Default	Your value
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 131. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 132. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 133. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 134. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Administrative agents for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 135. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 136. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Administrative agent

Table 137. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		

Table 137. Default Values (continued).

Enter your values:

Item		Default	Your value
	Set default names and userids based on cell and system identifiers	Not selected	
	Two-character cell identifier	AZ	
	Single-character system identifier	A	
Port defaults			
	Set default port values from the following port range	Not selected	
	Lowest default port number	9510	
	Highest default port number	9519	

Table 138. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 139. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 140. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		
User ID	WSADMIN	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2403	
WebSphere Application Server user ID home directory	/var/ WebSphere/ home	

Table 141. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
Daemon user ID		
User ID	WSDMNU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2434	

Table 142. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 143. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOADMA	
Long name	bboadma	
Node names		
Short name	BBOADMA	
Long name	bboadma	
Server names		
Short name	BBOADMA	
Long name	adminagent	adminagent
Cluster transition name	BBOADMA	

Table 144. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AdminAgent	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		
Hierarchical File System (HFS)	Not selected	
zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 145. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link		

Table 145. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 146. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOADMA.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 147. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO8GCR	
Servant process			
	Job name	server_short_nameS	server_short_nameS
	Procedure name	BBO8GSR	

Table 148. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	JMX SOAP connector port	8877	
ORB listener IP address		*	
	ORB listener port	9807	
	ORB SSL listener port	0	
HTTP transport IP address		*	

Table 148. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port	9630	

Table 149. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv85config/ cell_long_name/ node_long_name/Daemon	/wasv85config/cell_long_name/ node_long_name/ Daemon
Daemon job name	BBODMNG	
Procedure name	BBO8DMNG	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 150. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 151. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	

Table 151. Administrative Security Selection (continued).

Enter your values:

Item	Default	Your value
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 152. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 153. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 154. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 155. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for deployment managers

This article covers the requirements for a deployment manager.

About this task

When configuring your deployment manager node, keep the following in mind:

- When allocating target datasets for this option, it is possible, though not recommended, to use the same target datasets that you used for the standalone application server node. The job names for each configuration are very close to one another; and if you use the same target datasets, you might find it difficult to keep the two sets of jobs separate. Therefore, it is better to create a new set of target datasets and keep the two sets of jobs separate from one another.
- If possible, set up your file system such that the root file system is shared among all processors and the deployment manager's configuration is in a configuration HFS on a system-generic mount point.

Note: This configuration scenario is the best for certain tasks, such as starting the deployment manager on another system, that you might want to perform in the future.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in "z/OS customization variables: Deployment managers."
3. Save the worksheet for use during Network Deployment cell customization.

z/OS customization variables: Deployment managers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a deployment manager.

The WebSphere Application Server for z/OS runtime requires four servers in a Network Deployment cell: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a deployment manager.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type

Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on a cell identifier

When this option is selected, default cell, node, server, and procedure names as well as group names and user IDs are based on a cell identifier.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 20 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users**Common controller user ID****User ID**

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID**User ID**

User ID associated with the servant regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator**User ID**

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Configure Additional Users

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Daemon user ID**User ID**

User ID associated with the daemon

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the daemon user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMBOLS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMBOLS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Note: Each management server (administrative agent, deployment manager, or job manager) should be assigned its own cell name that is different from that of any other WebSphere Application Server cell on the same z/OS sysplex.

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names**Short name**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node
This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names**Short name**

Name that identifies the server to z/OS facilities such as SAF
The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server
This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Cluster transition name

WLM APPLENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System**Mount point**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmli member

CTRACE parmli member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmli member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port

Port number used by node agents to connect to this deployment manager server (CELL_DISCOVERY_ADDRESS)

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the `virtualhosts.xml` file, which makes setting a specific IP address here less than ideal. If you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port

Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port

Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager (DataPowerMgr_inbound_secure)

Middleware agent RPC port

Communications port for WebSphere Extended Deployment administrative functions (XDAGENT_PORT)

Administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_UDP_LISTENER_ADDRESS)

Administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_TCP_LISTENER_ADDRESS)

Status update listener port

Port that job managers and deployment managers listen on for status updates coming from registered nodes (STATUS_LISTENER_ADDRESS)

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All

RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

The port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization

Certificate authority keylabel

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,o=<company>,c=<country>

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1**Job statement 2****Job statement 3****Job statement 4****z/OS customization worksheet: Deployment managers for Version 7.0**

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this deployment manager:

System name: _____

Sysplex name: _____

Table 156. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 157. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Deployment manager

Table 158. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on a cell identifier	Not selected	
Two-character cell identifier	AZ	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9529	

Table 159. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 160. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 160. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSCFG1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2500
WebSphere Application Server servant group information			
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 161. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 162. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 163. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 164. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOCELL	
	Long name	bbocell	
Node names			
	Short name	BBODMGR	
	Long name	bbodmgr	
Server names			
	Short name	BBODMGR	
	Long name	dmgr	dmgr
Cluster transition name		BBODMGR	

Table 165. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	DeploymentManager	

Table 165. Configuration File System (continued).

Enter your values:

Item	Default	Your value
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
	Hierarchical File System (HFS)	Selected
	zSeries File System (ZFS)	Not selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 166. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe

Table 167. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmliib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOCELL.ERROR. LOG
CTRACE parmliib member		
	CTRACE parmliib member suffix (optional)	60

Table 168. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO7DCR
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO7DSR

Table 169. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		None
	JMX SOAP connector port	8879
	Cell discovery address port	7277
ORB listener IP address		*
	ORB listener port	9809
	ORB SSL listener port	0
HTTP transport IP address		*
	Administrative console port	9060
	Administrative console secure port	9043
Administrative interprocess communication port (K)		9632
High Availability Manager communication port (DCS)		9352
DataPower appliance manager secure inbound port		5555

Table 170. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv7config/ cell_long_name/ node_long_name/Daemon</i>	<i>/wasv7config/cell_long_name/ node_long_name/Daemon</i>
Daemon job name	BBODMNC	
Procedure name	BBO7DMNC	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5755	

Table 170. Location Service Daemon Definitions (continued).

Enter your values:

Item	Default	Your value
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 171. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Enable SSL on location service daemon	Selected	

Table 172. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 173. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 174. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	

Table 174. Security Managed by the WebSphere Family Product (continued).

Enter your values:

Item	Default	Your value
Password	None	

Table 175. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 176. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Deployment managers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this deployment manager:

System name: _____

Sysplex name: _____

Table 177. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 178. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Deployment manager

Table 179. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on a cell identifier	Not selected
	Two-character cell identifier	AZ
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9510
	Highest default port number	9529

Table 180. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 181. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 181. Configure Common Groups (continued).

Enter your values:

Item			Default	Your value
	Group		WSCFG1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2500	
WebSphere Application Server servant group information				
	Group		WSSR1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2501	
WebSphere Application Server local user group information				
	Group		WSCLGP	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2502	

Table 182. Configure Common Users.

Enter your values:

Item			Default	Your value
Common controller user ID				
	User ID		WSCRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2431	
Common servant user ID				
	User ID		WSSRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2432	
WebSphere Application Server administrator				
	User ID		WSADMIN	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2403	
WebSphere Application Server user ID home directory			/var/ WebSphere/ home	

Table 183. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 184. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 185. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOCELL	
	Long name	bbocell	
Node names			
	Short name	BBODMGR	
	Long name	bbodmgr	
Server names			
	Short name	BBODMGR	
	Long name	dmgr	dmgr
Cluster transition name		BBODMGR	

Table 186. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	DeploymentManager	

Table 186. Configuration File System (continued).

Enter your values:

Item	Default	Your value
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 187. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall

Table 188. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmliib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOCELL.ERROR. LOG
CTRACE parmliib member		
	CTRACE parmliib member suffix (optional)	60

Table 189. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8DCR
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8DSR

Table 190. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		None
	JMX SOAP connector port	8879
	Cell discovery address port	7277
ORB listener IP address		*
	ORB listener port	9809
	ORB SSL listener port	0
HTTP transport IP address		*
	Administrative console port	9060
	Administrative console secure port	9043
Administrative interprocess communication port		9632
High Availability Manager communication port (DCS)		9352
DataPower appliance manager secure inbound port		5555

Table 191. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv8config/ cell_long_name/ node_long_name/Daemon</i>	<i>/wasv8config/cell_long_name/ node_long_name/Daemon</i>
Daemon job name	BBODMNC	
Procedure name	BBO8DMNC	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5755	

Table 191. Location Service Daemon Definitions (continued).

Enter your values:

Item	Default	Your value
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 192. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 193. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 194. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 195. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 196. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 197. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Deployment managers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this deployment manager:

System name: _____

Sysplex name: _____

Table 198. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 199. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Deployment manager

Table 200. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on a cell identifier	Not selected
	Two-character cell identifier	AZ
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9510
	Highest default port number	9529

Table 201. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 202. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 202. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group		WSCFG1
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2500
WebSphere Application Server servant group information			
	Group		WSSR1
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group		WSCLGP
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 203. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID		WSCRU1
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID		WSSRU1
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID		WSADMIN
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 204. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 205. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 206. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOCELL	
	Long name	bbocell	
Node names			
	Short name	BBODMGR	
	Long name	bbodmgr	
Server names			
	Short name	BBODMGR	
	Long name	dmgr	dmgr
Cluster transition name		BBODMGR	

Table 207. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	DeploymentManager	

Table 207. Configuration File System (continued).

Enter your values:

Item	Default	Your value
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 208. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall

Table 209. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmliib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOCELL.ERROR. LOG
CTRACE parmliib member		
	CTRACE parmliib member suffix (optional)	60

Table 210. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8DCR
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8DSR

Table 211. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		
	JMX SOAP connector port	8879
	Cell discovery port	7277
ORB listener IP address		
	ORB listener port	9809
	ORB SSL listener port	0
HTTP transport IP address		
	Administrative console port	9060
	Administrative console secure port	9043
Administrative interprocess communication port		
High availability manager communication port (DCS)		
DataPower appliance manager secure inbound port		
Middleware agent RPC port		
Administration overlay UDP port		
Administration overlay TCP port		
Status update listener port		

Table 212. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv85config/ cell_long_name/ node_long_name/Daemon</i>	<i>/wasv85config/cell_long_name/ node_long_name/ Daemon</i>
Daemon job name	BBODMNC	

Table 212. Location Service Daemon Definitions (continued).

Enter your values:

Item	Default	Your value
Procedure name	BBO8DMNC	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 213. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring. <i>cell_short_name</i>	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 214. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 215. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	

Table 215. Security Managed by the z/OS Product (continued).

Enter your values:

Item	Default	Your value
Enable writable SAF keyring support	Not selected	

Table 216. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 217. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 218. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for new managed (custom) nodes

This article covers the requirements for a managed (custom) node.

Before you begin

You need to have already configured a Network Deployment cell and deployment manager.

About this task

Create a new managed node in a Network Deployment cell in order to add application servers to the cell.

This part of the configuration process creates an application server node structure, a node agent (for node administration), and a location service daemon (if one does not already exist) for the chosen z/OS system. This can be the same z/OS system on which the deployment manager was configured or a different z/OS system in the same sysplex. Once the managed node is created and federated into the Network Deployment cell, add application servers using the administrative console or scripting. You can use the configuration file system and user IDs created for the managed server node for the application servers in the node as well.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Managed (custom) nodes.”
3. Save the worksheet for use during managed node customization.

z/OS customization variables: Managed (custom) nodes

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a managed (custom) node.

During this customization task, you create a (temporary) cell configuration, a node configuration, and a (temporary) location service daemon.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Note: The cell configuration and location service daemon are temporary because they are replaced shortly after creation when the new node is federated.

The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for the future node agent and application servers.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and

it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell and system identifiers

When this option is selected, default cell, node, server, and procedure names as well as group names and user IDs are based on cell and system identifiers.

Two-character cell identifier

Two-character cell identifier (for the Network Deployment cell into which this node will be federated) to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

The port range must contain at least 10 ports.

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID

User ID

User ID associated with the servant and control adjunct regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator**User ID**

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Configure Additional Users

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Controller adjunct user ID**User ID**

User ID associated with the control adjunct

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control adjunct user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Daemon user ID**User ID**

User ID associated with the daemon

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the daemon user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMB0LS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMB0LS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Node Names

Note: A cell short name of BBOTEMP and a cell long name of bbotemp will be assigned to the unfederated managed node. These names will no longer be used after the managed node is federated into a Network Deployment cell.

Node names**Short name**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. If you plan to federate this application server into a Network Deployment cell, you might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 300 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member

CTRACE parmlib member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Process Definitions

Controller process

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Controller adjunct process

Procedure name

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must be seven or fewer characters.

Servant process

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new node, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

Target deployment manager does not reside in same sysplex**IP Name**

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization**Certificate authority keylabel**

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

You might want to set the managed node's SAF key ring name to be the same as that of the Network Deployment cell into which it will be federated.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as key stores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Federate Application Server

Application server access

WebSphere Application Server home directory path name

Home directory

Configuration file system mount point

Read/write file-system directory mount point where application data and environment files are written

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the application server configuration resides

Deployment manager access**Node host name or IP address**

IP name or address of the system on which the deployment manager server is configured

This value, equivalent to cell host in addNode.sh, is used by other WebSphere Application Server for z/OS functions to connect to this server in order to federate the designated node into the deployment manager cell.

The node host name must always resolve to an IP stack on the system where the deployment manager runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

Deployment manager JMX connection type

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port

JMX (Java Management Extensions) SOAP (Simple Object Access Protocol) connector port that the add-node request uses to connect to the deployment manager

It provides the federation process with knowledge of which deployment manager is the target of the federation.

Deployment manager connection requires security information

Indicates whether a user ID (and associated password) with full administration privileges is required to connect to the deployment manager

The user ID and password are required when global security is enabled on the Network Deployment cell unless an RMI connector is being used. If an RMI connector is being used, the identity information will be extracted from the thread of execution of the addNode job if the user ID and password are not specified.

User ID

User ID with full administrative privileges for the Network Deployment cell

Password

Password for the user ID that has full administrative privileges for the Network Deployment cell

Node agent definitions**Server name (short)**

Name of the node agent server

This is the server's jobname, as specified in the MVS START command JOBNAME parameter. This value identifies the server to certain z/OS facilities used by WebSphere Application Server for z/OS (SAF for example).

Rule: Name must contain seven or fewer all-uppercase characters.

Server name (long)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console. The node agent server long name is set to the fixed value of nodeagent.

Node host name

IP address or host name of the system on which the node resides

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

Node discovery port

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port

Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node middleware agent RPC port

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Node group name

Node group into which the node will be placed

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

Launch the node agent after node federation

Indicates whether the node agent is to be started automatically after federating a node

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Certificate**Default personal certificate****Issued to distinguished name**

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

`cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>`

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

`cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,o=<company>,c=<country>`

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1**Job statement 2****Job statement 3**

Job statement 4

z/OS customization worksheet: Managed (custom) nodes for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this managed (custom) node:

System name: _____

Sysplex name: _____

Table 219. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCustomxx	
Response file path name (optional)	None	

Table 220. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9550	
Highest default port number	9559	

Table 221. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 222. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server servant group information		
Group	WSSR1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2501	
WebSphere Application Server local user group information		
Group	WSCLGP	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2502	

Table 223. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		

Table 223. Configure Common Users (continued).

Enter your values:

Item		Default	Your value
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
Asynchronous administration user ID			
	User ID	WSADMSH	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2504
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 224. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Controller adjunct user ID			
	User ID	WSCRAU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2433
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 225. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 226. Node Names.

Enter your values:

Item	Default	Your value
Node names		
	Short name	BBONODE
	Long name	bbonode

Table 227. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
	Hierarchical File System (HFS)	Selected
	zSeries File System (ZFS)	Not selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	300	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 228. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe

Table 229. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOCELL.ERROR.LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 230. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Procedure name	BBO7ACR	
Controller adjunct process			
	Procedure name	BBO7CRA	
Servant process			
	Procedure name	BBO7ASR	
Admin asynch operations procedure name		BBO7ADM	

Table 231. Location Service Daemon Definitions.

Enter your values:

Item		Default	Your value
Daemon home directory		/wasv7config/ cell_long_name/ node_long_name/ Daemon	/wasv7config/cell_long_name/ node_long_name/Daemon
Daemon job name		BBODMNB	
Procedure name		BBO7DMNB	
Target deployment manager does not reside in same sysplex		Not selected	
	IP name	None	
	Listen IP	*	
	Port	5655	
	SSL port	5656	
	Register daemon with WLM DNS	Not selected	

Table 232. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	

Table 233. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 234. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value
Application server access		
	WebSphere Application Server home directory path name	
	Configuration file system mount point	/wasv7config/cell_long_name/node_long_name
	Directory path name relative to mount point	AppServer
Deployment manager access		
	Node host name or IP address	None
	Deployment manager JMX connection type	
	RMI	Not selected
	SOAP	Selected
	Deployment manager JMX port	8879
	Deployment manager connection requires security information	Not selected
	User ID	WSADMIN
	Password	None

Table 235. Federate Application Server (Part 2).

Enter your values:

Item	Default	Your value
Node agent definitions		

Table 235. Federate Application Server (Part 2) (continued).

Enter your values:

Item		Default	Your value
	Server name (short)	BBON001	
	Server name (long)	nodeagent	nodeagent
	Node host name	None	
	JMX SOAP connector port	8878	
	ORB listener IP address	*	
		ORB listener port	2810
		ORB SSL listener port	0
	Node discovery port	7272	
	Node multicast discovery port	5000	
	Node IPv6 multicast discovery port	5001	
	Administrative local port	9626	
	High Availability Manager communication port (DCS)	9354	
Node group name		DefaultNodeGroup	
Launch the node agent after federation		Selected	

Table 236. Security Certificate.

Enter your values:

Item		Default	Your value
Default personal certificate			
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Expiration period in years	1	
Root signing certificate			
	Expiration period in years	25	
Default keystore password			

Table 237. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Managed (custom) nodes for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this managed (custom) node:

System name: _____

Sysplex name: _____

Table 238. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCustomxx	
Response file path name (optional)	None	

Table 239. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		

Table 239. Default Values (continued).

Enter your values:

Item		Default	Your value
	Set default port values from the following port range	Not selected	
	Lowest default port number	9550	
	Highest default port number	9559	

Table 240. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 241. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 242. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		

Table 242. Configure Common Users (continued).

Enter your values:

Item		Default	Your value
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
Asynchronous administration user ID			
	User ID	WSADMSH	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2504
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 243. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Controller adjunct user ID			
	User ID	WSCRAU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2433
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 244. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 245. Node Names.

Enter your values:

Item	Default	Your value
Node names		
Short name	BBONODE	
Long name	bbonode	

Table 246. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	300	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 247. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		

Table 247. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall	

Table 248. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOCELL.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 249. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Procedure name	BBO8ACR	
Controller adjunct process			
	Procedure name	BBO8CRA	
Servant process			
	Procedure name	BBO8ASR	
Admin asynch operations procedure name		BBO8ADM	

Table 250. Location Service Daemon Definitions.

Enter your values:

Item		Default	Your value
Daemon home directory		/wasv8config/ cell_long_name/ node_long_name/ Daemon	/wasv8config/cell_long_name/ node_long_name/Daemon
Daemon job name		BBODMNB	
Procedure name		BBO8DMNB	

Table 250. Location Service Daemon Definitions (continued).

Enter your values:

Item		Default	Your value
Target deployment manager does not reside in same sysplex		Not selected	
	IP name	None	
	Listen IP	*	
	Port	5655	
	SSL port	5656	
	Register daemon with WLM DNS	Not selected	

Table 251. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	

Table 252. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 253. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value	
Application server access			
	WebSphere Application Server home directory path name		
	Configuration file system mount point	/wasv8config/ cell_long_name/ node_long_name	/wasv8config/cell_long_name/ node_long_name
	Directory path name relative to mount point	AppServer	AppServer
Deployment manager access			

Table 253. Federate Application Server (Part 1) (continued).

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
Deployment manager JMX connection type		
RMI	Not selected	
SOAP	Selected	
Deployment manager JMX port	8879	
Deployment manager connection requires security information	Not selected	
User ID	WSADMIN	
Password	None	

Table 254. Federate Application Server (Part 2).

Enter your values:

Item	Default	Your value
Node agent definitions		
Server name (short)	BBON001	
Server name (long)	nodeagent	nodeagent
Node host name	None	
JMX SOAP connector port	8878	
ORB listener IP address	*	
ORB listener port	2810	
ORB SSL listener port	0	
Node discovery port	7272	
Node multicast discovery port	5000	
Node IPv6 multicast discovery port	5001	
Administrative local port	9626	
High Availability Manager communication port (DCS)	9354	
Node group name	DefaultNodeGroup	
Launch the node agent after federation	Selected	

Table 255. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		

Table 255. Security Certificate (continued).

Enter your values:

Item	Default	Your value
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 256. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Managed (custom) nodes for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this managed (custom) node:

System name: _____

Sysplex name: _____

Table 257. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCustomxx	

Table 257. Customization Definition Name (continued).

Enter your values:

Item	Default	Your value
Response file path name (optional)	None	

Table 258. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9550
	Highest default port number	9559

Table 259. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 260. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
	Group	WSCFG1
	Allow OS security to assign GID	Not selected
	Assign user-specified GID	Selected
	Specified GID	2500
WebSphere Application Server servant group information		

Table 260. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 261. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 262. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
Controller adjunct user ID		

Table 262. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
	User ID	WSCRAU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2433
Daemon user ID			
	User ID	WSDMNU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2434

Table 263. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 264. Node Names.

Enter your values:

Item		Default	Your value
Node names			
	Short name	BBONODE	
	Long name	bbonode	

Table 265. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		

Table 265. Configuration File System (continued).

Enter your values:

Item		Default	Your value
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZHS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		300	
Secondary allocation in cylinders		100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.			

Table 266. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 267. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOCELL.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 268. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Procedure name	BBO8ACR	

Table 268. Process Definitions (continued).

Enter your values:

Item	Default	Your value
Controller adjunct process		
Procedure name	BBO8CRA	
Servant process		
Procedure name	BBO8ASR	

Table 269. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value	
Daemon home directory	/wasv85config/ cell_long_name/ node_long_name/ Daemon	/wasv85config/cell_long_name/ node_long_name/Daemon	
Daemon job name	BBODMNB		
Procedure name	BBO8DMNB		
Target deployment manager does not reside in same sysplex	Not selected		
	IP name	None	
	Listen IP	*	
	Port	5655	
	SSL port	5656	
	Register daemon with WLM DNS	Not selected	

Table 270. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	

Table 271. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 272. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value
Application server access		
	WebSphere Application Server home directory path name	
	Configuration file system mount point	/wasv85config/ cell_long_name/ node_long_name
	Directory path name relative to mount point	AppServer
Deployment manager access		
	Node host name or IP address	None
	Deployment manager JMX connection type	
	RMI	Not selected
	SOAP	Selected
	Deployment manager JMX port	8879
	Deployment manager connection requires security information	Not selected
	User ID	WSADMIN
	Password	None

Table 273. Federate Application Server (Part 2).

Enter your values:

Item	Default	Your value
Node group name	DefaultNodeGroup	
Launch the node agent after federation	Selected	
Enable writable SAF keyring support	Not selected	
Node agent definitions		

Table 273. Federate Application Server (Part 2) (continued).

Enter your values:

Item		Default	Your value
	Server name (short)	BBON001	
	Server name (long)	nodeagent	nodeagent
	Node host name	None	
	JMX SOAP connector port	8878	
	ORB listener IP address	*	
	ORB listener port	2810	
	ORB SSL listener port	0	
	Node discovery port	7272	
	Node multicast discovery port	5000	
	Node IPv6 multicast discovery port	5001	
	Node agent interprocess communication port	9626	
	High availability manager communication port (DCS)	9354	
	Middleware agent RPC port	7061	
	Administration overlay UDP port	11001	
	Administration overlay TCP port	11002	

Table 274. Security Certificate.

Enter your values:

Item		Default	Your value
Default personal certificate			
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Expiration period in years	1	
Root signing certificate			
	Expiration period in years	25	
Default keystore password			

Table 275. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning to federate standalone servers into a Network Deployment cells

Before you begin

You must have configured a Network Deployment cell (and deployment manager) and a standalone application server. The two need to have a common MVS group and user domain and reside within the same z/OS sysplex.

About this task

Federate an existing standalone application server node into a Network Deployment cell in order to add application servers to the cell. The Deployment Manager needs to be at an equal or higher service level than the node being federated.

The cell structure and location service daemon for the standalone application server are discarded. The standalone application server node and its application servers become a new node in the Network Deployment cell. The standalone application server's configuration file system and home directory stay in use, but are modified to reflect the new cell name. New symbolic links for use during server startup are added.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Federating application servers.”
3. Save the worksheet for use during federated application server node customization.

z/OS customization variables: Federating application servers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to federate an application server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as `config_hlq`) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Federate Application Server

Application server access

WebSphere Application Server home directory path name

Home directory

Configuration file system mount point

Read/write file-system directory mount point where application data and environment files are written

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the application server configuration resides

Application server security is enabled

Indicates whether global security is enabled on the cell containing the application server

User ID

User ID with full administrative privileges for the cell containing the application server

Password

Password for the user ID that has full administrative privileges for the cell containing the application server

Deployment manager access

Node host name or IP address

IP name or address of the system on which the deployment manager server is configured

This value, equivalent to cell host in `addNode.sh`, is used by other WebSphere Application Server for z/OS functions to connect to this server in order to federate the designated node into the deployment manager cell.

The node host name must always resolve to an IP stack on the system where the deployment manager runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

Deployment manager JMX connection type

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port

JMX (Java Management Extensions) SOAP (Simple Object Access Protocol) connector port that the add-node request uses to connect to the deployment manager

It provides the federation process with knowledge of which deployment manager is the target of the federation.

Deployment manager connection requires security information

Indicates whether a user ID (and associated password) with full administration privileges is required to connect to the deployment manager

The user ID and password are required when global security is enabled on the Network Deployment cell unless an RMI connector is being used. If an RMI connector is being used, the identity information will be extracted from the thread of execution of the addNode job if the user ID and password are not specified.

User ID

User ID with full administrative privileges for the Network Deployment cell

Password

Password for the user ID that has full administrative privileges for the Network Deployment cell

Node agent definitions

Server name (short)

Name of the node agent server

This is the server's jobname, as specified in the MVS START command JOBNAME parameter. This value identifies the server to certain z/OS facilities used by WebSphere Application Server for z/OS (SAF for example).

Rule: Name must contain seven or fewer all-uppercase characters.

Server name (long)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console. The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

Node discovery port

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port

Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node middleware agent RPC port

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Application server's new ORB listener port

Port for IOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IOP requests

This user ID also owns all of the configuration file systems.

Rule: Value cannot be 0.

Node group name

Node group into which the node will be placed

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

Configuration group name

Group name of the WebSphere Application Server configuration group

Configuration user ID

User ID that owns the configuration file system

Include apps

Indicates whether to include applications with your deployment manager node

Enabling this option instructs the **addNode** command to include applications from the node; otherwise, it would remove them prior to federation. If the application already exists in the cell, a warning is printed and the application is not installed into the cell.

You must use this option to migrate all of the applications to the new cell. Federating the node to a cell using the **addNode** command does not merge any cell-level configuration information, including that from virtualHost.

Launch the node agent after node federation

Indicates whether the node agent is to be started automatically after federating a node

Federate service integration busses that exist on this node

Indicates whether to federate service integration busses that exist on this node

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

z/OS customization worksheet: Federating application servers for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this federated node:

System name: _____

Sysplex name: _____

Table 276. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZFederatexx	
Response file path name (optional)	None	

Table 277. Default Values.

Enter your values:

Item	Default	Your value
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9550
	Highest default port number	9559

Table 278. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 279. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value
Application server access		
WebSphere Application Server home directory path name		
	Configuration file system mount point	/wasv7config
	Directory path name relative to mount point	AppServer
	Application server security is enabled	Not selected
	Local user ID	None
	Local password	None
Deployment manager access		
	Node host name or IP address	None
Deployment manager JMX connection type		
	RMI	Not selected
	SOAP	Selected
	Deployment manager JMX port	8879
	Deployment manager connection requires security information	Not selected
	User ID	WSADMIN
	Password	None

Table 280. Federate Application Server (Part 2).

Enter your values:

Item	Default	Your value
Node agent definitions		
	Server name (short)	BBON001
	Server name (long)	nodeagent
	JMX SOAP connector port	8878
	ORB listener IP address	*
	ORB listener port	2810
	ORB SSL listener port	0
	Node discovery port	7272
	Node multicast discovery port	5000
	Node IPv6 multicast discovery port	5001
	Administrative local port	9626
	High Availability Manager communication port (DCS)	9354
	Application server's new ORB listener port	9810

Table 280. Federate Application Server (Part 2) (continued).

Enter your values:

Item	Default	Your value
Node group name	DefaultNodeGroup	
Configuration group name	WSCFG1	
Configuration user ID	WSADMIN	
Include apps	Selected	
Launch the node agent after federation	Selected	
Federate service integration busses that exist on the node	Not selected	

Table 281. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Federating application servers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this federated node:

System name: _____

Sysplex name: _____

Table 282. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZFederatexx	
Response file path name (optional)	None	

Table 283. Default Values.

Enter your values:

Item	Default	Your value
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9550
	Highest default port number	9559

Table 284. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 285. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value
Application server access		
	WebSphere Application Server home directory path name	
	Configuration file system mount point	/wasv8config
	Directory path name relative to mount point	AppServer
	Application server security is enabled	Not selected
	Local user ID	None
	Local password	None
Deployment manager access		
	Node host name or IP address	None
	Deployment manager JMX connection type	
	RMI	Not selected
	SOAP	Selected
	Deployment manager JMX port	8879
	Deployment manager connection requires security information	Not selected
	User ID	WSADMIN
	Password	None

Table 286. Federate Application Server (Part 2).

Enter your values:

Item	Default	Your value
Node agent definitions		
Server name (short)	BBON001	
Server name (long)	nodeagent	nodeagent
JMX SOAP connector port	8878	
ORB listener IP address	*	
	ORB listener port	2810
	ORB SSL listener port	0
Node discovery port	7272	
Node multicast discovery port	5000	
Node IPv6 multicast discovery port	5001	
Administrative local port	9626	
High Availability Manager communication port (DCS)	9354	
Application server's new ORB listener port	9810	
Node group name	DefaultNodeGroup	
Configuration group name	WSCFG1	
Configuration user ID	WSADMIN	
Include apps	Selected	
Launch the node agent after federation	Selected	
Federate service integration busses that exist on the node	Not selected	

Table 287. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Federating application servers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this federated node: _____

System name: _____

Sysplex name: _____

Table 288. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZFederatexx	
Response file path name (optional)	None	

Table 289. Default Values.

Enter your values:

Item	Default	Your value
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9550
	Highest default port number	9559

Table 290. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 291. Federate Application Server (Part 1).

Enter your values:

Item	Default	Your value
Application server access		
	WebSphere Application Server home directory path name	
	Configuration file system mount point	/wasv85config
	Directory path name relative to mount point	AppServer
	Application server security is enabled	Not selected
	Local user ID	None
	Local password	None
Deployment manager access		

Table 291. Federate Application Server (Part 1) (continued).

Enter your values:

Item		Default	Your value
	Node host name or IP address	None	
	Deployment manager JMX connection type		
	RMI	Not selected	
	SOAP	Selected	
	Deployment manager JMX port	8879	
	Deployment manager connection requires security information	Not selected	
	User ID	WSADMIN	
	Password	None	

Table 292. Federate Application Server (Part 2).

Enter your values:

Item		Default	Your value
	Application server's new ORB listener port	9810	
	Node group name	DefaultNodeGroup	
	Configuration group name	WSCFG1	
	Configuration user ID	WSADMIN	
	Include apps	Selected	
	Launch the node agent after federation	Selected	
	Federate service integration busses that exist on the node	Not selected	
Node agent definitions			
	Server name (short)	BBON001	
	Server name (long)	nodeagent	nodeagent
	JMX SOAP connector port	8878	
	ORB listener IP address	*	
	ORB listener port	2810	
	ORB SSL listener port	0	
	Node discovery port	7272	
	Node multicast discovery port	5000	
	Node IPv6 multicast discovery port	5001	
	Node agent interprocess communication port	9626	
	High availability manager communication port (DCS)	9354	
	Middleware agent RPC port	7061	
	Administration overlay UDP port	11001	
	Administration overlay TCP port	11002	

Table 293. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for Network Deployment cells with application servers

This article covers the requirements for a Network deployment cells with application servers.

About this task

A Network Deployment cell is a full-function WebSphere Application Server for z/OS configuration on which you can deploy and run applications. A Network Deployment cell with application server includes the following:

- Cell configuration
- Deployment manager that runs the administrative console application
- Single location service daemon on each z/OS system
- One application server consisting of a node agent and one application server
- One or more application server nodes (one is recommended) on each z/OS target system hosting portions of the cell. Each node consists of a node agent and some number of application servers

This part of the configuration process creates the initial cell configuration, the deployment manager, and a location service daemon for the z/OS system, plus a node agent with an application server. Once the Network Deployment cell is created, you can add additional application server nodes by creating and federating new managed nodes, or by federating standalone application server nodes into the Network Deployment cell.

When configuring your deployment manager node, set up your file system such that the root file system is shared among all processors and the deployment manager's configuration is in a configuration file system on a system-generic mount point.

Note: This configuration scenario is the best for certain tasks, such as starting the deployment manager on another system, that you might want to perform in the future.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Network Deployment cells with application servers.”
3. Save the worksheet for use during Network Deployment cell with an application server customization.

z/OS customization variables: Network Deployment cells with application servers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a Network Deployment cell with an application server.

The WebSphere Application Server for z/OS runtime requires four standalone cell servers: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a Network Deployment cell with an application server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell, cluster, and system identifiers

When this option is selected, default cell, node, server, cluster, and procedure names as well as group names and user IDs are based on cell, cluster, and system identifiers.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Two-character cluster identifier

Two-character cluster identifier to be used to create default names and user IDs

Rule: The characters must be alphabetic characters. The alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 50 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID

User ID

User ID associated with the servant and control adjunct regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator

User ID

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Deployment manager node names

Short name

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Deployment manager server names**Short name**

Name that identifies the server to z/OS facilities such as SAF

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Node agent and application server node names**Short name**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Node agent server names**Short name**

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Application server names

Short name

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Deployment manager cluster transition name

WLM APPLENV (WLM application environment) name for the deployment manage

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Application server cluster transition name

WLM APPLENV (WLM application environment) name for the application server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Deployment Manager Configuration File System

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

Deployment Manager Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli b member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmli b member

CTRACE parmli b member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmli b member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmli b member in the SBBOJCL dataset can be used to create this CTRACE parmli b member.

Application Server Configuration File System

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Optional Application Deployment

Deploy the administrative console

Specify whether to install a Web-based administrative console that manages the application server.

Deploying the administrative console is recommended, but if you deselect this option, the information center contains detailed steps for deploying it after the profile exists.

Deploy the default application

Specify whether to install the default application that contains the Snoop, Hello, and HitCount servlets.

Process Definitions

Deployment manager controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Deployment manager servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Application server controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Application server controller adjunct process

Job name

Job name used by WLM to start the application server control region adjunct

This is set to the server short name followed by the letter A, and it cannot be changed through the tool.

Procedure name

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must be seven or fewer characters.

Application server servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment

Deployment manager ports:

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port

Port number used by node agents to connect to this deployment manager server (CELL_DISCOVERY_ADDRESS)

ORB listener IP address

IP address on which the server's ORB listens for incoming IOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IOP requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IOP requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the `virtualhosts.xml` file, which makes setting a specific IP address here less than ideal. If you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port

Port for HTTP requests to the administrative console

Administrative console secure port

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (K)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (`DCS_UNICAST_ADDRESS`)

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager (`DataPowerMgr_inbound_secure`)

Middleware agent RPC port

Communications port for WebSphere Extended Deployment administrative functions (`XDAGENT_PORT`)

Administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (`OVERLAY_UDP_LISTENER_ADDRESS`)

Administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (`OVERLAY_TCP_LISTENER_ADDRESS`)

Status update listener port

Port that job managers and deployment managers listen on for status updates coming from registered nodes (`STATUS_LISTENER_ADDRESS`)

Rule: Value cannot be 0.

Node agent ports:

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (`SOAP_CONNECTOR_ADDRESS`)

JMX is used for remote administrative functions, such as invoking scripts through `wsadmin.sh`.

Rule: Value cannot be 0.

ORB listener port

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests (`BOOTSTRAP_ADDRESS` and `ORB_LISTENER_ADDRESS`)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOP requests (`ORB_SSL_LISTENER_ADDRESS`)

The default is 0, which allows the system to choose this port.

Node agent interprocess communication port (K)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

Node discovery port

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port

Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Node middleware agent RPC port

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Application server ports:

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB listener port

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport port

Port for HTTP requests (WC_defaulthost)

Rule: Value cannot be 0.

HTTPS transport port

Port for secure HTTP requests (WC_defaulthost_secure)

Rule: Value cannot be 0.

Administrative local port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (DCS)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

Service integration port

Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration secure port

Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability port

Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability secure port

Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Session initiation protocol (SIP) port

Port for session initiation requests (SIP_DEFAULTHOST)

Rule: Value cannot be 0.

Session initiation protocol (SIP) secure port

Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Rule: Value cannot be 0.

Administration overlay UDP port

UDP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_UDP_LISTENER_ADDRESS)

Administration overlay TCP port

TCP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_TCP_LISTENER_ADDRESS)

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but once chosen, it is difficult to change, even in the middle of customization.

SSL port

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization

Certificate authority keylabel

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

Internally, this sets SecurityDomainType to the string "cellQualified". All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Web Server Definition

Create a web server definition

Indicates whether to create a web server definition.

Web server type

Select the web server type from the list of supported web servers.

Web server operating system

Operating system where the web server is located

Web server name

Name used in defining the web server to WebSphere Application Server

Web server host name or IP address

IP name or address of the system on which the web server is located

Web server port

HTTP port on which the web server listens

Web server installation directory path

Name of the directory where the web server is installed

Web server plug-in installation directory path

Name of the directory where the web server plug-ins are installed

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Network Deployment cells with application servers for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this cell:

System name: _____

Sysplex name: _____

Table 294. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCellxx	
Response file path name (optional)	None	

Table 295. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell, cluster, and system identifiers	Not selected
	Two-character cell identifier	AZ
	Two-character cluster identifier	00
	Single-character system identifier	A
Port defaults		

Table 295. Default Values (continued).

Enter your values:

Item		Default	Your value
	Set default port values from the following port range	Not selected	
	Lowest default port number	9510	
	Highest default port number	9559	

Table 296. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 297. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2500	
WebSphere Application Server servant group information			
	Group	WSSR1	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2501	
WebSphere Application Server local user group information			
	Group	WSCLGP	
	Allow OS security to assign GID	Not selected	
	Assign user-specified GID	Selected	
	Specified GID	2502	

Table 298. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		

Table 298. Configure Common Users (continued).

Enter your values:

Item		Default	Your value
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
Asynchronous administration user ID			
	User ID	WSADMSH	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2504
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 299. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 300. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOCELL	
	Long name	bbocell	
Deployment manager node names			

Table 300. Cell, Node, and Server Names (continued).

Enter your values:

Item		Default	Your value
	Short name	BBODMGR	
	Long name	bbodmgr	
Deployment manager server names			
	Short name	BBODMGR	
	Long name	dmgr	dmgr
Node agent and application server node names			
	Short name	BBONODE	
	Long name	bbonode	
Node agent server names			
	Short name	BBON001	
	Long name	nodeagent	nodeagent
Application server names			
	Short name	BBOS001	
	Long name	server1	
Deployment manager cluster transition name		BBODMGR	
Application server cluster transition name		BBOC001	
JVM mode			
	31 bit	Not selected	
	64 bit	Selected	

Table 301. Deployment Manager Configuration File System.

Enter your values:

Item		Default	Your value
Mount point		/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point		DeploymentManager	
Dataset name		OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type			
	Hierarchical File System (HFS)	Selected	
	zSeries File System (ZFS)	Not selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

Table 302. Deployment Manager Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe	

Table 303. Application Server Configuration File System.

Enter your values:

Item		Default	Your value
Mount point		/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point		AppServer	
Dataset name		OMVS.WAS70.cell_ short_name. node_short_name.HFS	
File system type			
	Hierarchical File System (HFS)	Selected	
	zSeries File System (ZFS)	Not selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	

Table 304. Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ nodeagent_long_ name/ wassmpe	

Table 305. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOCELL.ERROR.LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 306. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	
Deploy the default application	Selected	
Deploy the sample applications	Not selected	

Table 307. Process Definitions.

Enter your values:

Item		Default	Your value
Deployment manager controller process			
	Job name	<i>server_short_name</i>	<i>server_short_name</i>
	Procedure name	BBO7DCR	
Deployment manager servant process			
	Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
	Procedure name	BBO7DSR	
Application server controller process			
	Job name	<i>server_short_name</i>	<i>server_short_name</i>
	Procedure name	BBO7ACR	
Application server controller adjunct process			
	Job name	<i>server_short_nameA</i>	<i>server_short_nameA</i>
	Procedure name	BBO7CRA	
Application server servant process			
	Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
	Procedure name	BBO7ASR	
Admin asynch operations procedure name		BBO7ADM	

Table 308. Port Values Assignment.

Enter your values:

Item	Default	Your value
Deployment manager ports		
Node host name or IP address	None	
JMX SOAP connector port	8879	
Cell discovery address port	7277	
ORB listener IP address	*	
ORB listener port	9809	
ORB SSL listener port	0	
HTTP transport IP address	*	
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port (K)	9632	
High Availability Manager communication port (DCS)	9352	
DataPower appliance manager secure inbound port	5555	
Node agent ports		
JMX SOAP connector port	8878	
ORB listener port	2810	
ORB SSL listener port	0	
Node agent interprocess communication port (K)	9626	
High Availability Manager communication port (DCS)	9354	
Node discovery port	7272	
Node multicast discovery port	5000	
Node IPv6 multicast discovery port	5001	
Application server ports		
JMX SOAP connector port	8880	
ORB listener port	2809	
ORB SSL listener port	0	
HTTP transport port	9080	
HTTPS transport port	9443	
Administrative local port	9633	
High Availability Manager communication port (DCS)	9353	

Table 308. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Service integration port	7276	
Service integration secure port	7286	
Service integration MQ interoperability port	5558	
Service integration MQ interoperability secure port	5578	
Session initiation protocol (SIP) port	5060	
Session initiation protocol (SIP) secure port	5061	

Table 309. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv7config/ cell_long_name/ dngr_node_long_name/ Daemon	/wasv7config/cell_long_name/ dngr_node_long_name/ Daemon
Daemon job name	BBODMNC	
Procedure name	BBO7DMNC	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 310. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Enable SSL on location service daemon	Selected	

Table 311. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	

Table 311. Administrative Security Selection (continued).

Enter your values:

Item	Default	Your value
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 312. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	<i>cell_short_name</i>	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 313. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	
Sample applications		
User name	samples	samples
Password	None	

Table 314. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	<i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Issued by distinguished name	<i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i>	
Expiration period in years	1	
Root signing certificate		

Table 314. Security Certificate (continued).

Enter your values:

Item		Default	Your value
	Expiration period in years	25	
Default keystore password			

Table 315. Web Server Definition (Part 1).

Enter your values:

Item		Default	Your value
Create a web server definition		Not selected	
	Web server type	IBM HTTP Server	
	Web server operating system	z/OS	
	Web server name	webserver1	
	Web server host name or IP address	<i>host_name</i>	
	Web server port	80	

Table 316. Web Server Definition (Part 2).

Enter your values:

Item	Default	Your value
Web server installation directory path	/etc/websrv1	
Web server plug-in installation directory path	/etc/websrv1/Plugins	

Table 317. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Network Deployment cells with application servers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this cell:

System name: _____

Sysplex name: _____

Table 318. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCellxx	
Response file path name (optional)	None	

Table 319. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell, cluster, and system identifiers	Not selected	
Two-character cell identifier	AZ	
Two-character cluster identifier	00	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9559	

Table 320. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 321. Configure Common Groups.

Enter your values:

Item		Default	Your value
WebSphere Application Server configuration group information			
	Group	WSCFG1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2500
WebSphere Application Server servant group information			
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 322. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
Asynchronous administration user ID			

Table 322. Configure Common Users (continued).

Enter your values:

Item		Default	Your value
	User ID	WSADMSH	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2504
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 323. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 324. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOCELL	
	Long name	bbocell	
Deployment manager node names			
	Short name	BBODMGR	
	Long name	bbodmgr	
Deployment manager server names			
	Short name	BBODMGR	
	Long name	dmgr	dmgr
Node agent and application server node names			
	Short name	BBONODE	
	Long name	bbonode	
Node agent server names			
	Short name	BBON001	
	Long name	nodeagent	nodeagent
Application server names			
	Short name	BBOS001	
	Long name	server1	
Deployment manager cluster transition name		BBODMGR	
Application server cluster transition name		BBOC001	

Table 325. Deployment Manager Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	DeploymentManager	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 326. Deployment Manager Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall

Table 327. Application Server Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	AppServer	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS	
File system type		

Table 327. Application Server Configuration File System (continued).

Enter your values:

Item		Default	Your value
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	

Table 328. Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ nodeagent_long_name/ wasInstall	

Table 329. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOCELL.ERROR.LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 330. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	

Table 330. Optional Application Deployment (continued).

Enter your values:

Item	Default	Your value
Deploy the default application	Selected	

Table 331. Process Definitions.

Enter your values:

Item	Default	Your value
Deployment manager controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8DCR
Deployment manager servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8DSR
Application server controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8ACR
Application server controller adjunct process		
	Job name	<i>server_short_nameA</i>
	Procedure name	BBO8CRA
Application server servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8ASR
Admin asynch operations procedure name		
		BBO8ADM

Table 332. Port Values Assignment.

Enter your values:

Item	Default	Your value
Deployment manager ports		
Node host name or IP address		None
	JMX SOAP connector port	8879
	Cell discovery address port	7277
ORB listener IP address		*
	ORB listener port	9809
	ORB SSL listener port	0
HTTP transport IP address		*

Table 332. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port	9632	
High Availability Manager communication port (DCS)	9352	
DataPower appliance manager secure inbound port	5555	
Application server ports		
JMX SOAP connector port	8880	
ORB listener port	2809	
ORB SSL listener port	0	
HTTP transport port	9080	
HTTPS transport port	9443	
Administrative local port	9633	
High Availability Manager communication port (DCS)	9353	
Service integration port	7276	
Service integration secure port	7286	
Service integration MQ interoperability port	5558	
Service integration MQ interoperability secure port	5578	
Session initiation protocol (SIP) port	5060	
Session initiation protocol (SIP) secure port	5061	
Node agent ports		
JMX SOAP connector port	8878	
ORB listener port	2810	
ORB SSL listener port	0	
Node agent interprocess communication port	9626	
High Availability Manager communication port (DCS)	9354	
Node discovery port	7272	
Node multicast discovery port	5000	
Node IPv6 multicast discovery port	5001	

Table 333. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv8config/ cell_long_name/ dngr_node_long_name/ Daemon	/wasv8config/cell_long_name/ dngr_node_long_name/ Daemon
Daemon job name	BBODMNC	
Procedure name	BBO8DMNC	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 334. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 335. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 336. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		

Table 336. Security Managed by the z/OS Product (continued).

Enter your values:

Item	Default	Your value
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 337. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 338. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 339. Web Server Definition (Part 1).

Enter your values:

Item	Default	Your value
Create a web server definition	Not selected	

Table 339. Web Server Definition (Part 1) (continued).

Enter your values:

Item	Default	Your value
Web server type	IBM HTTP Server	
Web server operating system	z/OS	
Web server name	webserver1	
Web server host name or IP address	host_name	
Web server port	80	

Table 340. Web Server Definition (Part 2).

Enter your values:

Item	Default	Your value
Web server installation directory path	/etc/websrv1	
Web server plug-in installation directory path	/etc/websrv1/Plugins	

Table 341. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Network Deployment cells with application servers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this cell:

System name: _____

Sysplex name: _____

Table 342. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZCellxx	
Response file path name (optional)	None	

Table 343. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell, cluster, and system identifiers	Not selected	
Two-character cell identifier	AZ	
Two-character cluster identifier	00	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9559	

Table 344. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 345. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 345. Configure Common Groups (continued).

Enter your values:

Item			Default	Your value
	Group		WSCFG1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2500	
WebSphere Application Server servant group information				
	Group		WSSR1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2501	
WebSphere Application Server local user group information				
	Group		WSCLGP	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2502	

Table 346. Configure Common Users.

Enter your values:

Item			Default	Your value
Common controller user ID				
	User ID		WSCRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2431	
Common servant user ID				
	User ID		WSSRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2432	
WebSphere Application Server administrator				
	User ID		WSADMIN	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2403	
WebSphere Application Server user ID home directory			/var/ WebSphere/ home	

Table 347. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 348. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
	Short name	BBOCELL
	Long name	bbocell
Deployment manager node names		
	Short name	BBODMGR
	Long name	bbodmgr
Deployment manager server names		
	Short name	BBODMGR
	Long name	dmgr
Node agent and application server node names		
	Short name	BBONODE
	Long name	bbonode
Node agent server names		
	Short name	BBON001
	Long name	nodeagent
Application server names		
	Short name	BBOS001
	Long name	server1
Deployment manager cluster transition name	BBODMGR	
Application server cluster transition name	BBOC001	

Table 349. Deployment Manager Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	DeploymentManager	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	

Table 349. Deployment Manager Configuration File System (continued).

Enter your values:

Item		Default	Your value
File system type			
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.			

Table 350. Deployment Manager Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 351. Application Server Configuration File System.

Enter your values:

Item		Default	Your value
Mount point		/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point		AppServer	
Dataset name		OMVS.WAS85.cell_ short_name. node_short_name.ZFS	
File system type			
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	

Table 352. Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ nodeagent_long_name/ wasInstall

Table 353. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOCELL.ERROR. LOG
CTRACE parmli member		
	CTRACE parmli member suffix (optional)	60

Table 354. Optional Application Deployment.

Enter your values:

Item	Default	Your value
Deploy the administrative console	Selected	
Deploy the default application	Selected	

Table 355. Process Definitions.

Enter your values:

Item	Default	Your value
Deployment manager controller process		
	Job name	server_short_name
	Procedure name	BBO8DCR
Deployment manager servant process		
	Job name	server_short_nameS
	Procedure name	BBO8DSR

Table 355. Process Definitions (continued).

Enter your values:

Item	Default	Your value
Application server controller process		
Job name	<i>server_short_name</i>	<i>server_short_name</i>
Procedure name	BBO8ACR	
Application server controller adjunct process		
Job name	<i>server_short_nameA</i>	<i>server_short_nameA</i>
Procedure name	BBO8CRA	
Application server servant process		
Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
Procedure name	BBO8ASR	

Table 356. Port Values Assignment.

Enter your values:

Item	Default	Your value
Deployment manager ports		
Node host name or IP address	None	
JMX SOAP connector port	8879	
Cell discovery address port	7277	
ORB listener IP address	*	
ORB listener port	9809	
ORB SSL listener port	0	
HTTP transport IP address	*	
Administrative console port	9060	
Administrative console secure port	9043	
Administrative interprocess communication port	9632	
High Availability Manager communication port (DCS)	9352	
DataPower appliance manager secure inbound port	5555	
Middleware agent RPC port	7060	
Administration overlay UDP port	11005	
Administration overlay TCP port	11006	
Status update listener port	9420	
Node agent ports		
JMX SOAP connector port	8878	
ORB listener port	2810	

Table 356. Port Values Assignment (continued).

Enter your values:

Item	Default	Your value
ORB SSL listener port	0	
Node agent interprocess communication port	9626	
High availability manager communication port (DCS)	9354	
Node discovery port	7272	
Node multicast discovery port	5000	
Node IPv6 multicast discovery port	5001	
Middleware agent RPC port	7061	
Administration overlay UDP port	11001	
Administration overlay TCP port	11002	
Application server ports		
JMX SOAP connector port	8880	
ORB listener port	2809	
ORB SSL listener port	0	
HTTP transport port	9080	
HTTPS transport port	9443	
Administrative interprocess communication port	9633	
High Availability Manager communication port (DCS)	9353	
Service integration port	7276	
Service integration secure port	7286	
Service integration MQ interoperability port	5558	
Service integration MQ interoperability secure port	5578	
Session initiation protocol (SIP) port	5060	
SIP secure port	5061	
Administration overlay UDP port	11003	
Administration overlay TCP port	11004	

Table 357. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv85config/ cell_long_name/ dngr_node_long_name/ Daemon	/wasv85config/cell_long_name/ dngr_node_long_name/ Daemon
Daemon job name	BBODMNC	
Procedure name	BBO8DMNC	
IP name	host_name	

Table 357. Location Service Daemon Definitions (continued).

Enter your values:

Item	Default	Your value
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 358. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 359. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 360. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 361. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 362. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 363. Web Server Definition (Part 1).

Enter your values:

Item	Default	Your value
Create a web server definition		Not selected
	Web server type	IBM HTTP Server
	Web server operating system	z/OS
	Web server name	webserver1
	Web server host name or IP address	host_name
	Web server port	80

Table 364. Web Server Definition (Part 2).

Enter your values:

Item	Default	Your value
Web server installation directory path	/etc/websrv1	
Web server plug-in installation directory path	/etc/websrv1/Plugins	

Table 365. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for job managers

A job manager allows you to submit administrative jobs asynchronously for application servers registered to administrative agents and for deployment managers. You can submit these jobs to a large number of servers over a geographically dispersed area.

About this task

Use the WebSphere Customization Toolbox or the `zpmf` command and the customization jobs that they generate to configure a job manager on z/OS. The job manager does not have to run on the same system as the nodes that it manages.

After the job manager is up and running, you can make the following types of servers known to a job manager through a registration process:

- Application servers registered to administrative agents
You can register standalone application server nodes with an administrative agent. You can then register one or more of the nodes with a job manager.
- Deployment managers

After you register the servers, you can queue administrative jobs directed at the application servers or deployment managers through the job manager.

The job manager allows you to asynchronously administer job submissions. You can perform the following tasks:

- Set a job submission to take effect at a specified time.
- Set a job submission to expire at a specified time.
- Schedule a job submission to occur at a specified time interval.
- Notify the administrator through email that a job has completed.

For more information, read the *Administering nodes using the job manager* article in the information center.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Job managers.”
3. Save the worksheet for use during job manager customization.

z/OS customization variables: Job managers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a job manager.

The WebSphere Application Server for z/OS runtime requires four servers in a Network Deployment cell: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a deployment manager.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type

Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on a cell and system identifiers

When this option is selected, default cell, node, server, and procedure names as well as group names and user IDs are based on cell and system identifiers.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID

User ID

User ID associated with the servant region

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator

User ID

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Configure Additional Users

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Daemon user ID

User ID

User ID associated with the daemon

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the daemon user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMBOLS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMBOLS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Note: Each management server (administrative agent, deployment manager, or job manager) should be assigned its own cell name that is different from that of any other WebSphere Application Server cell on the same z/OS sysplex.

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell
This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names**Short name**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node
This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names**Short name**

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Cluster transition name

WLM APPLENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member

CTRACE parmlib member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Servant process

Job name

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB listener IP address

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal. If you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port

Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port

Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Status update listener port

Port that job managers and deployment managers listen on for status updates coming from registered nodes (STATUS_LISTENER_ADDRESS)

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOp IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

The port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization**Certificate authority keylabel**

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Job managers for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this job manager:

System name: _____

Sysplex name: _____

Table 366. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	
Response file path name (optional)	None	

Table 367. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Job manager

Table 368. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9519	

Table 369. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 370. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server servant group information		

Table 370. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 371. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 372. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item	Default	Your value
Daemon user ID		

Table 372. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 373. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 374. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Node names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Server names			
	Short name	BBOJMGR	
	Long name	jobmgr	jobmgr
Cluster transition name		BBOJMGR	

Table 375. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	JobManager	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	

Table 375. Configuration File System (continued).

Enter your values:

Item		Default	Your value
File system type			
	Hierarchical File System (HFS)	Selected	
	zSeries File System (ZFS)	Not selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

Table 376. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe	

Table 377. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOJMGR.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 378. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			

Table 378. Process Definitions (continued).

Enter your values:

Item		Default	Your value
	Job name	<i>server_short_name</i>	<i>server_short_name</i>
	Procedure name	BBO7JCR	
Servant process			
	Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
	Procedure name	BBO7JSR	

Table 379. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	JMX SOAP connector port	8876	
ORB listener IP address		*	
	ORB listener port	9808	
	ORB SSL port	0	
HTTP transport IP address		*	
	Administrative console port	9960	
	Administrative console secure port	9943	
Administrative interprocess communication port (K)		9631	

Table 380. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv7config/cell_long_name/node_long_name/Daemon</i>	<i>/wasv7config/cell_long_name/node_long_name/Daemon</i>
Daemon job name	BBODMNJ	
Procedure name	BBO7DMNJ	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5855	
SSL port	5856	
Register daemon with WLM DNS	Not selected	

Table 381. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Enable SSL on location service daemon	Selected	

Table 382. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 383. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 384. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 385. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		

Table 385. Security Certificate (continued).

Enter your values:

Item	Default	Your value
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 386. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Job managers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this job manager:

System name: _____

Sysplex name: _____

Table 387. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	

Table 387. Customization Definition Name (continued).

Enter your values:

Item	Default	Your value
Response file path name (optional)	None	

Table 388. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Job manager

Table 389. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9519	

Table 390. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 391. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 391. Configure Common Groups (continued).

Enter your values:

Item			Default	Your value
	Group		WSCFG1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2500	
WebSphere Application Server servant group information				
	Group		WSSR1	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2501	
WebSphere Application Server local user group information				
	Group		WSCLGP	
		Allow OS security to assign GID	Not selected	
		Assign user-specified GID	Selected	
		Specified GID	2502	

Table 392. Configure Common Users.

Enter your values:

Item			Default	Your value
Common controller user ID				
	User ID		WSCRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2431	
Common servant user ID				
	User ID		WSSRU1	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2432	
WebSphere Application Server administrator				
	User ID		WSADMIN	
		Allow OS security to assign UID	Not selected	
		Assign user-specified UID	Selected	
		Specified UID	2403	
WebSphere Application Server user ID home directory			/var/ WebSphere/ home	

Table 393. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 394. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 395. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Node names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Server names			
	Short name	BBOJMGR	
	Long name	jobmgr	jobmgr
Cluster transition name		BBOJMGR	

Table 396. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	JobManager	

Table 396. Configuration File System (continued).

Enter your values:

Item	Default	Your value
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 397. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall

Table 398. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOJMGR.ERROR. LOG
CTRACE parmli member		
	CTRACE parmli member suffix (optional)	60

Table 399. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8JCR
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8JSR

Table 400. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		None
	JMX SOAP connector port	8876
ORB listener IP address		*
	ORB listener port	9808
	ORB SSL listener port	0
HTTP transport IP address		*
	Administrative console port	9960
	Administrative console secure port	9943
Administrative interprocess communication port		9631

Table 401. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv8config/ cell_long_name/ node_long_name/Daemon</i>	<i>/wasv8config/cell_long_name/ node_long_name/Daemon</i>
Daemon job name	BBODMNJ	
Procedure name	BBO8DMNJ	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5855	
SSL port	5856	
Register daemon with WLM DNS	Not selected	

Table 402. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 403. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 404. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 405. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 406. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 407. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Job managers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this job manager:

System name: _____

Sysplex name: _____

Table 408. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZManagementxx	

Table 408. Customization Definition Name (continued).

Enter your values:

Item	Default	Your value
Response file path name (optional)	None	

Table 409. Server Type Selection.

Enter your values:

Item	Default	Your value
Server type	Deployment manager	Job manager

Table 410. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9519	

Table 411. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 412. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		

Table 412. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSCFG1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2500
WebSphere Application Server servant group information			
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 413. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 414. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

Item		Default	Your value
Daemon user ID			
	User ID	WSDMNU1	
	Allow OS security to assign UID	Not selected	
	Assign user-specified UID	Selected	
	Specified UID	2434	

Table 415. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 416. Cell, Node, and Server Names.

Enter your values:

Item		Default	Your value
Cell names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Node names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Server names			
	Short name	BBOJMGR	
	Long name	jobmgr	jobmgr
Cluster transition name		BBOJMGR	

Table 417. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	JobManager	

Table 417. Configuration File System (continued).

Enter your values:

Item	Default	Your value
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 418. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link		
	Create intermediate symbolic link	Selected
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall

Table 419. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmliib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item	Default	Your value
Error log stream		
	Error log stream name (optional)	BBOJMGR.ERROR. LOG
CTRACE parmliib member		
	CTRACE parmliib member suffix (optional)	60

Table 420. Process Definitions.

Enter your values:

Item	Default	Your value
Controller process		
	Job name	<i>server_short_name</i>
	Procedure name	BBO8JCR
Servant process		
	Job name	<i>server_short_nameS</i>
	Procedure name	BBO8JSR

Table 421. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address		None
	JMX SOAP connector port	8876
ORB listener IP address		*
	ORB listener port	9808
	ORB SSL listener port	0
HTTP transport IP address		*
	Administrative console port	9960
	Administrative console secure port	9943
Administrative interprocess communication port		9631
Status update listener port		9425

Table 422. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv85config/cell_long_name/node_long_name/Daemon</i>	<i>/wasv85config/cell_long_name/node_long_name/Daemon</i>
Daemon job name	BBODMNJ	
Procedure name	BBO8DMNJ	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5855	
SSL port	5856	
Register daemon with WLM DNS	Not selected	

Table 423. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 424. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 425. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	cell_short_name	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 426. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 427. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US
	Expiration period in years	1
Root signing certificate		
	Expiration period in years	25
Default keystore password		

Table 428. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for secure proxy servers

You can create a secure proxy server on a node in a demilitarized zone (DMZ). The DMZ zone is a safe zone between firewalls that is typically located between the client and the backend server.

About this task

Use the WebSphere Customization Toolbox or the `zpm` command and the customization jobs that they generate to configure a secure proxy server on z/OS.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Secure proxy servers.”
3. Save the worksheet for use during secure proxy server customization.

z/OS customization variables: Secure proxy servers

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a secure proxy server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell and system identifiers

When this option is selected, default cell, node, server, cluster, and procedure names as well as group names and user IDs are based on cel and system identifiers.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs (provides minimal access to the cell)

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users**Common controller user ID****User ID**

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID**User ID**

User ID associated with the servant and control adjunct regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator**User ID**

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names**System name**

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMBOLS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMBOLS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names**Cell names****Short name**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell
This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names**Short name**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node
This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names**Short name**

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server job name.

Rules: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name

WLM APPL ENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPL ENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. You might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read "Product file system" on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member

CTRACE parmlib member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Security Level Selection

Select the security level setting for this proxy server and choose the protocols to support.

Proxy security level

High Represents the highest level of proxy server security based on certain proxy server settings

Medium

Represents the mid-level of proxy server security based on certain proxy server settings

Low

Represents the lowest level of proxy server security based on certain proxy server settings

Supported protocols

Web Select to support web protocol

SIP Select to support SIP protocol

Port Values Assignment

Node host name or IP address

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

Bootstrap port

Port for IIOp requests that acts as the bootstrap port for this server

Rule: Value cannot be 0.

HTTP transport IP address

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

HTTP transport port

Port for HTTP requests (WC_defaulthost)

Rule: Value cannot be 0.

HTTPS transport port

Port for secure HTTP requests (WC_defaulthost_secure)

Rule: Value cannot be 0.

Session initiation protocol (SIP) port

Port for session initiation requests (SIP_DEFAULTHOST)

Rule: Value cannot be 0.

Session initiation protocol (SIP) secure port

Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Rule: Value cannot be 0.

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for enterprise beans for example) establish connections to the location service daemon first, then forward them to the target server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization

Certificate authority keylabel

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Secure proxy servers for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this secure proxy server:

System name: _____

Sysplex name: _____

Table 429. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZProxyxx	
Response file path name (optional)	None	

Table 430. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9520
	Highest default port number	9529

Table 431. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 432. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server local user group information		
Group	WSCLGP	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2502	

Table 433. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		
User ID	WSADMIN	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2403	
Asynchronous administration user ID		
User ID	WSADMSH	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2504	
WebSphere Application Server user ID home directory	/var/ WebSphere/ home	

Table 434. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 435. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
	Short name	BBOPROX
	Long name	bboprox
Node names		
	Short name	BBOPROX
	Long name	bboprox
Server names		
	Short name	BBOPROX
	Long name	proxy1
Cluster transition name		BBOPROX

Table 436. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxy	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
	Hierarchical File System (HFS)	Selected
	zSeries File System (ZFS)	Not selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 437. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere_SPS/ V7R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe	

Table 438. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmlib member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPROX.ERROR. LOG	
CTRACE parmlib member			
	CTRACE parmlib member suffix (optional)	60	

Table 439. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO7XCR	
Admin asynch operations procedure name		BBO7ADM	

Table 440. Security Level Selection.

Enter your values:

Item		Default	Your value
Proxy security level			
	High	Selected	
	Medium	Not selected	
	Low	Not selected	
Supported protocols			

Table 440. Security Level Selection (continued).

Enter your values:

Item		Default	Your value
	Web	Selected	
	SIP	Selected	

Table 441. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	Bootstrap port	2809	
HTTP transport IP address		*	
	HTTP transport port	80	
	HTTPS transport port	443	
Session initiation protocol (SIP) port		5060	
Session initiation protocol (SIP) secure port		5061	
Administrative interprocess communication port (K)		9633	

Table 442. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	wasv7config/ cell_long_name/ node_long_name/Daemon	wasv7config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNX	
Procedure name	BBO7DMNX	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 443. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	

Table 443. SSL Customization (continued).

Enter your values:

Item	Default	Your value
Default SAF keyring name	WASKeyring.cell_ short_name	
Enable SSL on location service daemon	Selected	

Table 444. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 445. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 446. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 447. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Secure proxy servers for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this secure proxy server:

System name: _____

Sysplex name: _____

Table 448. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZProxyxx	
Response file path name (optional)	None	

Table 449. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9520
	Highest default port number	9529

Table 450. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 451. Configure Common Groups.

Enter your values:

Item	Default		Your value
WebSphere Application Server configuration group information			
	Group		WSCFG1
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2500
WebSphere Application Server local user group information			
	Group		WSCLGP
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 452. Configure Common Users.

Enter your values:

Item	Default		Your value
Common controller user ID			
	User ID		WSCRU1
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID		WSSRU1
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID		WSADMIN
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
Asynchronous administration user ID			
	User ID		WSADMSH
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2504
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 453. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 454. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
	Short name	BBOPROX
	Long name	bboprox
Node names		
	Short name	BBOPROX
	Long name	bboprox
Server names		
	Short name	BBOPROX
	Long name	proxy1
Cluster transition name		BBOPROX

Table 455. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxy	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 456. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere_SPS/V8R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall	

Table 457. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPROX.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 458. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO8XCR	
Admin asynch operations procedure name		BBO8ADM	

Table 459. Security Level Selection.

Enter your values:

Item		Default	Your value
Proxy security level			
	High	Selected	
	Medium	Not selected	
	Low	Not selected	
Supported protocols			

Table 459. Security Level Selection (continued).

Enter your values:

Item		Default	Your value
	Web	Selected	
	SIP	Selected	

Table 460. Port Values Assignment.

Enter your values:

Item		Default	Your value
Node host name or IP address		None	
	Bootstrap port	2809	
HTTP transport IP address		*	
	HTTP transport port	80	
	HTTPS transport port	443	
Session initiation protocol (SIP) port		5060	
Session initiation protocol (SIP) secure port		5061	
Administrative interprocess communication port		9633	

Table 461. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	wasv8config/ cell_long_name/ node_long_name/Daemon	wasv8config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNX	
Procedure name	BBO8DMNX	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 462. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	

Table 462. SSL Customization (continued).

Enter your values:

Item	Default	Your value
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 463. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 464. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 465. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 466. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	

Table 466. Job Statement Definition (continued).

Enter your values:

Item	Default	Your value
//*	//*	

z/OS customization worksheet: Secure proxy servers for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this secure proxy server:

System name: _____

Sysplex name: _____

Table 467. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZProxyxx	
Response file path name (optional)	None	

Table 468. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9520
	Highest default port number	9529

Table 469. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 470. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server local user group information		
Group	WSCLGP	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2502	

Table 471. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		
User ID	WSADMIN	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2403	
WebSphere Application Server user ID home directory	/var/ WebSphere/ home	

Table 472. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 473. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
	Short name	BBOPROX
	Long name	bboprox
Node names		
	Short name	BBOPROX
	Long name	bboprox
Server names		
	Short name	BBOPROX
	Long name	proxy1
Cluster transition name		BBOPROX

Table 474. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxy	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		
	Hierarchical File System (HFS)	Not selected
	zSeries File System (ZFS)	Selected
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 475. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere_SPS/V8R5	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 476. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPROX.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 477. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO8XCR	

Table 478. Security Level Selection.

Enter your values:

Item		Default	Your value
Proxy security level			
	High	Selected	
	Medium	Not selected	
	Low	Not selected	
Supported protocols			
	Web	Selected	
	SIP	Selected	

Table 479. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
Bootstrap port	2809	
HTTP transport IP address	*	
HTTP transport port	80	
HTTPS transport port	443	
Session initiation protocol (SIP) port	5060	
SIP secure port	5061	
Administrative interprocess communication port	9633	

Table 480. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	wasv85config/ cell_long_name/ node_long_name/Daemon	wasv85config/cell_long_name/ node_long_name/ Daemon
Daemon job name	BBODMNX	
Procedure name	BBO8DMNX	
IP name	host_name	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

Table 481. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 482. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 483. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 484. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 485. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for secure proxy administrative agents

A secure proxy administrative agent provides a single interface to administer multiple secure proxy servers.

About this task

An administrative agent can monitor and control multiple servers on one or more nodes. By using a single interface to administer your servers, you reduce the overhead of running administrative services in every server.

Use the WebSphere Customization Toolbox or the `zpm` command and the customization jobs that they generate to configure a secure proxy administrative agent on z/OS. The secure proxy administrative agent does not run an administrative console application; instead, it accepts commands through scripting or from a job manager with which it is registered. The administrative agent must run on the same z/OS system as the secure proxy servers that it manages, and it must use the same SAF configuration group as the servers to be managed.

After the administrative agent is up and running, you can use the following commands to register and unregister a secure proxy server node with the administrative agent:

- **registerNode**

Run the `registerNode` command to register a node with the administrative agent. When you run the command, the standalone node is converted into a node that the administrative agent manages. The administrative agent and the node being registered must be on the same system. You can only run the command on an unfederated node. If the command is run on a federated node, the command exits with an error.

Any node registered with the administrative agent automatically becomes eligible to register with the job manager.

- **deregisterNode**

Use the `deregisterNode` command to deregister a node from an administrative agent so that you can use the node standalone or register the node with another administrative agent. The node must have been previously registered with the administrative agent. When you deregister a node, the node configuration is retained but is marked as not registered with the administrative agent.

An administrative agent can register any of the profiles that it manages with a job manager.

For more information, read the *Administering nodes using the administrative agent* article in the information center.

Restrictions: If global security is enabled, the following restrictions apply to the administrative agent:

- - From the administrative console:
 - You will not see the status of the proxy servers.
 - You will not be able to start or stop the proxy servers. Use the command-line tools instead.
 - You cannot use runtime tabs to make changes to the running proxy servers.
- From scripting, you will not be able to use the AdminControl scripting object to make changes to the proxy servers.

Caution: Keep your environment secure. Do not disable administrative security to work around the restrictions.

Procedure

1. Print a copy of the customization worksheet.
2. Fill out the worksheet as described in “z/OS customization variables: Secure proxy administrative agents” on page 389.
3. Save the worksheet for use during secure proxy administrative agent customization.

z/OS customization variables: Secure proxy administrative agents

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a secure proxy administrative agent.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is not created, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Tip: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

Read “Configuration Planning Spreadsheets for z/OS” on page 111 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

Set each default GID and UID value to indicate that operating-system security is to assign an unused value

When this option is selected, each GID and UID value will be defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value will be defaulted to an IBM-provided number.

Name and userid defaults

Set default names and user IDs based on cell and system identifiers

When this option is selected, default cell, node, server, and procedure names as well as group names and user IDs are based on a cell and system identifiers.

Two-character cell identifier

Two-character cell identifier to be used to create default names and user IDs

Rule: The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

Single-character system identifier

Single-character system identifier to be used to create default names and user IDs

Rule: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults

Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number

Lowest number that may be assigned as a default port number

Highest default port number

Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as `config_hlq`) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the servant group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Assign user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the local user group

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Common servant user ID

User ID

User ID associated with the servant and control adjunct regions

If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server administrator

User ID

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

System name

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) is, use the console command D SYMBOLS on the target z/OS system to display it.

Sysplex name

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command D SYMBOLS on the target z/OS system to display it.

PROCLIB dataset name

Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

Short name

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long name

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names

Short name

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long name

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names**Short name**

Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long name

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rule: Name must be 50 or fewer characters.

Cluster transition name

WLM APPLENV (WLM application environment) name for this server

If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

Configuration File System**Mount point**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point

Relative path name of the directory within the configuration file system in which the configuration resides

Dataset name

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

File system type

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)

This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)

This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS

DASD volume serial number to contain the above dataset or * to let SMS select a volume

Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders

Initial size allocation in cylinders for the configuration file system dataset

Tip: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders

Size of each secondary extent in cylinders

Tip: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

Product file system directory

Name of the directory where WebSphere Application Server for z/OS files reside after installation

This is the SMP/E installation directory.

Read “Product file system” on page 20 for more information.

Intermediate symbolic link

Select this option to allow to set up an intermediate symbolic link, and specify the path name of that link if you select it

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link

Path name of intermediate symbolic link

Error Log Stream and CTRACE Parmlib Member

This panel only displays if you click **Window > Preferences > Profile Management Tool**, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Error log stream

Error log stream name (optional)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmli member

CTRACE parmli member suffix (optional)

Value that is appended to CTIBBO to form the name of the CTRACE parmli member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmli member in the SBBOJCL dataset can be used to create this CTRACE parmli member.

Process Definitions

Controller process

Job name

Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the control region

Rule: Name must be seven or fewer characters.

Servant process**Job name**

Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter S, and it cannot be changed through the tool.

Procedure name

Name of member in your procedure library to start the servant regions

Rule: Name must be seven or fewer characters.

Port Values Assignment**Node host name or IP address**

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

JMX SOAP connector port

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Bootstrap port

Port for IIOP requests that acts as the bootstrap port for this server (BOOTSTRAP_ADDRESS)

Rule: Value cannot be 0.

Administrative interprocess communication port

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Location Service Daemon Definitions

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name

Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

IP Name

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default value is your node host name.

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port

The port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS

If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL Customization**Certificate authority keylabel**

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate

Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates

Expiration date used for any X509 Certificate Authority certificates, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers

You must specify this even if you did not select the option to generate a certificate authority (CA) certificate.

Default SAF keyring name

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients

Select this option if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon

Select this option if you want to support secure communications using Inter-ORB Request Protocol (IROP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the guest user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Assign user-specified UID

Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Rule: UID values must be unique numeric values between 1 and 2,147,483,647.

Enable writable SAF keyring support

Select this option if you want to enable writable SAF key ring support

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name

User name for the administrator

Password

Password for the administrator

Rule: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name

Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name

Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,  
o=<company>,c=<country>
```

Expiration period in years

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password

Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

z/OS customization worksheet: Secure proxy administrative agents for Version 7.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 486. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAdminAgentxx	

Table 486. Customization Definition Name (continued).

Enter your values:

Item	Default	Your value
Response file path name (optional)	None	

Table 487. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
	Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected
Name and userid defaults		
	Set default names and userids based on cell and system identifiers	Not selected
	Two-character cell identifier	AZ
	Single-character system identifier	A
Port defaults		
	Set default port values from the following port range	Not selected
	Lowest default port number	9510
	Highest default port number	9519

Table 488. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 489. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
	Group	WSCFG1
	Allow OS security to assign GID	Not selected
	Assign user-specified GID	Selected
	Specified GID	2500
WebSphere Application Server servant group information		

Table 489. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 490. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 491. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 492. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOPRXA	
Long name	bboprxa	
Node names		
Short name	BBOPRXA	
Long name	bboprxa	
Server names		
Short name	BBOPRXA	
Long name	adminagent	adminagent
Cluster transition name	BBOPRXA	

Table 493. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv7config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxyAdmin	
Dataset name	OMVS.WAS70.cell_ short_name. node_short_name.HFS *	
File system type		
Hierarchical File System (HFS)	Selected	
zSeries File System (ZFS)	Not selected	
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.		

Table 494. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	
Intermediate symbolic link		

Table 494. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv7config/ cell_long_name/ node_long_name/ wassmpe	

Table 495. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPRXA.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 496. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO7YCR	
Servant process			
	Job name	server_short_nameS	server_short_nameS
	Procedure name	BBO7YSR	

Table 497. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
JMX SOAP connector port	8877	
Administrative interprocess communication port (K)	9630	

Table 498. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv7config/ cell_long_name/ node_long_name/Daemon	/wasv7config/cell_long_name/ node_long_name/Daemon
Daemon job name	BBODMNY	
Procedure name	BBO7DMNY	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 499. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Enable SSL on location service daemon	Selected	

Table 500. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 501. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		

Table 501. Security Managed by the z/OS Product (continued).

Enter your values:

Item	Default	Your value
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 502. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 503. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 504. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Secure proxy administrative agents for Version 8.0

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 505. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAdminAgentxx	
Response file path name (optional)	None	

Table 506. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9519	

Table 507. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 508. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server servant group information		
Group	WSSR1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2501	
WebSphere Application Server local user group information		
Group	WSCLGP	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2502	

Table 509. Configure Common Users.

Enter your values:

Item	Default	Your value
Common controller user ID		
User ID	WSCRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2431	
Common servant user ID		
User ID	WSSRU1	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2432	
WebSphere Application Server administrator		

Table 509. Configure Common Users (continued).

Enter your values:

Item	Default	Your value
User ID	WSADMIN	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
Specified UID	2403	
WebSphere Application Server user ID home directory	/var/ WebSphere/ home	

Table 510. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 511. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOPRXA	
Long name	bboprxa	
Node names		
Short name	BBOPRXA	
Long name	bboadma	
Server names		
Short name	BBOPRXA	
Long name	adminagent	adminagent
Cluster transition name	BBOPRXA	

Table 512. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv8config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxyAdmin	
Dataset name	OMVS.WAS80.cell_ short_name. node_short_name.ZFS *	

Table 512. Configuration File System (continued).

Enter your values:

Item		Default	Your value
File system type			
	Hierarchical File System (HFS)	Not selected	
	zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS		*	
Primary allocation in cylinders		420	
Secondary allocation in cylinders		100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.			

Table 513. WebSphere Application Server Product File System.

Enter your values:

Item		Default	Your value
Product file system directory		/usr/lpp/ zWebSphere/ V8R0	
Intermediate symbolic link			
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv8config/ cell_long_name/ node_long_name/ wasInstall	

Table 514. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPRXA.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 515. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			

Table 515. Process Definitions (continued).

Enter your values:

Item		Default	Your value
	Job name	<i>server_short_name</i>	<i>server_short_name</i>
	Procedure name	BBO8YCR	
Servant process			
	Job name	<i>server_short_nameS</i>	<i>server_short_nameS</i>
	Procedure name	BBO8YSR	

Table 516. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
JMX SOAP connector port	8877	
Administrative interprocess communication port (K)	9630	

Table 517. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	<i>/wasv8config/ cell_long_name/ node_long_name/Daemon</i>	<i>/wasv8config/cell_long_name/ node_long_name/Daemon</i>
Daemon job name	BBODMNY	
Procedure name	BBO8DMNY	
IP name	<i>host_name</i>	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 518. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring. <i>cell_short_name</i>	

Table 518. SSL Customization (continued).

Enter your values:

Item	Default	Your value
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 519. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 520. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		
	User ID	WSGUEST
	Allow OS security to assign UID	Not selected
	Assign user-specified UID	Selected
	UID	2402
Enable writable SAF keyring support	Not selected	

Table 521. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 522. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		

Table 522. Security Certificate (continued).

Enter your values:

Item		Default	Your value
	Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
	Expiration period in years	1	
Root signing certificate			
	Expiration period in years	25	
Default keystore password			

Table 523. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

z/OS customization worksheet: Secure proxy administrative agents for Version 8.5

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this administrative agent:

System name: _____

Sysplex name: _____

Table 524. Customization Definition Name.

Enter your values:

Item	Default	Your value
Customization definition name	ZAdminAgentxx	

Table 524. Customization Definition Name (continued).

Enter your values:

Item	Default	Your value
Response file path name (optional)	None	

Table 525. Default Values.

Enter your values:

Item	Default	Your value
GID and UID defaults		
Set each default GID and UID value to indicate OS security is to assign an unused value	Not selected	
Name and userid defaults		
Set default names and userids based on cell and system identifiers	Not selected	
Two-character cell identifier	AZ	
Single-character system identifier	A	
Port defaults		
Set default port values from the following port range	Not selected	
Lowest default port number	9510	
Highest default port number	9519	

Table 526. Target Datasets.

Enter your values:

Item	Default	Your value
High-level qualifier (HLQ)	None	

Table 527. Configure Common Groups.

Enter your values:

Item	Default	Your value
WebSphere Application Server configuration group information		
Group	WSCFG1	
Allow OS security to assign GID	Not selected	
Assign user-specified GID	Selected	
Specified GID	2500	
WebSphere Application Server servant group information		

Table 527. Configure Common Groups (continued).

Enter your values:

Item		Default	Your value
	Group	WSSR1	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2501
WebSphere Application Server local user group information			
	Group	WSCLGP	
		Allow OS security to assign GID	Not selected
		Assign user-specified GID	Selected
		Specified GID	2502

Table 528. Configure Common Users.

Enter your values:

Item		Default	Your value
Common controller user ID			
	User ID	WSCRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2431
Common servant user ID			
	User ID	WSSRU1	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2432
WebSphere Application Server administrator			
	User ID	WSADMIN	
		Allow OS security to assign UID	Not selected
		Assign user-specified UID	Selected
		Specified UID	2403
WebSphere Application Server user ID home directory		/var/ WebSphere/ home	

Table 529. System and Dataset Names.

Enter your values:

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	

Table 530. Cell, Node, and Server Names.

Enter your values:

Item	Default	Your value
Cell names		
Short name	BBOPRXA	
Long name	bboprxa	
Node names		
Short name	BBBOPRXA	
Long name	bboprxa	
Server names		
Short name	BBOPRXA	
Long name	adminagent	adminagent
Cluster transition name	BBOPRXA	

Table 531. Configuration File System.

Enter your values:

Item	Default	Your value
Mount point	/wasv85config/ cell_long_name/ node_long_name	
Directory path name relative to mount point	SecureProxyAdmin	
Dataset name	OMVS.WAS85.cell_ short_name. node_short_name.ZFS *	
File system type		
Hierarchical File System (HFS)	Not selected	
zSeries File System (ZFS)	Selected	
Volume, or '*' for SMS	*	
Primary allocation in cylinders	420	
Secondary allocation in cylinders	100	
* If you select the Hierarchical File System, you might want to change the extension of this file to .HFS.		

Table 532. WebSphere Application Server Product File System.

Enter your values:

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V8R5	
Intermediate symbolic link		

Table 532. WebSphere Application Server Product File System (continued).

Enter your values:

Item		Default	Your value
	Create intermediate symbolic link	Selected	
	Path name of intermediate symbolic link	/wasv85config/ cell_long_name/ node_long_name/ wasInstall	

Table 533. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in the WebSphere Customization Toolbox, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

Item		Default	Your value
Error log stream			
	Error log stream name (optional)	BBOPRXA.ERROR. LOG	
CTRACE parmli member			
	CTRACE parmli member suffix (optional)	60	

Table 534. Process Definitions.

Enter your values:

Item		Default	Your value
Controller process			
	Job name	server_short_name	server_short_name
	Procedure name	BBO8YCR	
Servant process			
	Job name	server_short_nameS	server_short_nameS
	Procedure name	BBO8YSR	

Table 535. Port Values Assignment.

Enter your values:

Item	Default	Your value
Node host name or IP address	None	
JMX SOAP connector port	8877	
Administrative interprocess communication port	9630	

Table 536. Location Service Daemon Definitions.

Enter your values:

Item	Default	Your value
Daemon home directory	/wasv85config/ cell_long_name/ node_long_name/Daemon	/wasv85config/cell_long_name/ node_long_name/ Daemon
Daemon job name	BBODMNY	
Procedure name	BBO8DMNY	
IP name	host_name	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

Table 537. SSL Customization.

Enter your values:

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Generate certificate authority (CA) certificate	Selected	
Expiration date for certificates	12/31/2021	
Default SAF keyring name	WASKeyring.cell_ short_name	
Use virtual keyring for z/OS SSL clients	Not selected	
Enable SSL on location service daemon	Selected	

Table 538. Administrative Security Selection.

Enter your values:

Item	Default	Your value
Use a z/OS security product	Selected	
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Table 539. Security Managed by the z/OS Product.

Enter your values:

Item	Default	Your value
SAF profile prefix	None	
WebSphere Application Server unauthenticated user		

Table 539. Security Managed by the z/OS Product (continued).

Enter your values:

Item	Default	Your value
User ID	WSGUEST	
Allow OS security to assign UID	Not selected	
Assign user-specified UID	Selected	
UID	2402	
Enable writable SAF keyring support	Not selected	

Table 540. Security Managed by the WebSphere Family Product.

Enter your values:

Item	Default	Your value
User name	WSADMIN	
Password	None	

Table 541. Security Certificate.

Enter your values:

Item	Default	Your value
Default personal certificate		
Issued to distinguished name	cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Issued by distinguished name	cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US	
Expiration period in years	1	
Root signing certificate		
Expiration period in years	25	
Default keystore password		

Table 542. Job Statement Definition.

Enter your values:

Item	Default	Your value
//jobname JOB	(ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM	
//*	//*	
//*	//*	
//*	//*	

Planning for recovery

About this task

This article helps you plan for any recovery measures that you might need to take.

Procedure

1. Decide whether or not to implement automatic restart. See “Automatic restart management (ARM)” on page 421 for more information.
2. Review the recommendations for starting a deployment manager on a different MVS image. See “Starting deployment managers on a different MVS image” for more information.

Starting deployment managers on a different MVS image

This describes steps you must follow to start your deployment manager on an MVS image different from the one on which it was originally configured.

About this task

The ability to start your deployment manager on an MVS image different from the one on which it was originally configured is handy if your original system becomes unavailable, either through a planned outage or a system failure. This way, you can still start and stop applications, make configuration updates, utilize monitors that use the PMI interface, perform other control functions, and so on. Perform the following steps to start your deployment manager on a different MVS image and ensure that client requests will successfully find the deployment manager at its new location.

Note: This works only if the deployment manager on the original MVS image is down. WebSphere Application Server for z/OS allows only one copy of the deployment manager to run at one time for any given cell.

Procedure

1. Ensure that the MVS image to which you are moving the deployment manager contains a node that is already part of the cell of the deployment manager you want to move.
2. Ensure that the location service daemon on the MVS image to which you are moving the deployment manager is up and running before you move the deployment manager.
3. Using the Profile Management Tool or `zpm` command, set your host names and ports appropriately:
 - Ensure that the host names and ports for the deployment manager are not specific to a particular system.
 - Ensure that you use a DVIPA generic host name, rather than a system-specific host name, for the node host name and an asterisk (“*”) for both the ORB listener IP address and HTTP transport IP address.
 - Consider configuring a secondary DVIPA in case the system with the primary VIPA is down.
4. Ensure that Sysplex Distributor is enabled so that, regardless of where the DVIPA has moved, it automatically routes any inbound traffic to the deployment manager.
5. Ensure that access to the PROCLIB is the same for both the original MVS image and the MVS image to which you want to move the deployment manager.
6. Start the deployment manager on the new system.

There are three ways to accomplish this, depending on the configuration of your HFSs. Follow the scenario that matches your configuration.

- Scenario 1: Root HFS is shared among all processors, deployment manager's configuration is in a configuration HFS on a system-generic mount point.

Issue the start command for the deployment manager on the system on which you want it to reside:

- To start the server in 31-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>
```

- To start the server in 64-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>,AMODE=64
```

- Scenario 2: Root HFS is shared among all processors, deployment manager's configuration HFS is mounted under a system-specific directory.

Note: This is an undesirable scenario that you should try to avoid from the start of your system configuration. If you find yourself with this setup, however, follow these steps for the workaround.

- Create a symbolic link at the equivalent system-specific location on the target MVS image. The contents of the symbolic link should point back to the actual mount point, which means you should not use \$SYSNAME anywhere.
- Issue the start command for the deployment manager on the system on which you want it to reside:
 - To start the server in 31-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>
```

- To start the server in 64-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>,AMODE=64
```

- Scenario 3: Root HFS is not shared among any processors, deployment manager's configuration HFS is mounted and accessible to only one system at a time.
 - Unmount the configuration HFS from the original MVS image and remount it (at a mount point with the same name) on the new MVS image.
 - Issue the start command for the deployment manager on the system on which you want it to reside:
 - To start the server in 31-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>
```

- To start the server in 64-bit mode:

```
S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortcode>.<node_shortcode>.<server_shortcode>,AMODE=64
```

Results

You know you are done when your deployment manager is up and running on a different MVS image and you are able to use it to make configuration updates to your environment.

Automatic restart management (ARM)

WebSphere Application Server for z/OS uses the z/OS automatic restart management (ARM) to recover application servers. Each application server running on a z/OS system (including servers you create for your business applications) are automatically registered with an ARM group. Each registration uses a special element type called SYSCB, which ARM treats as restart level 3, assuring that RRS restarts before any application server.

If you have an application that is critical for your business, you need facilities to manage failures. z/OS provides rich automation interfaces, such as ARM, that you can use to detect and recover from failures. ARM handles the restarting of servers when failures occur.

Tips:

- If you have ARM enabled on your system, you might want to disable ARM for the WebSphere Application Server for z/OS address spaces before you install and customize WebSphere Application Server for z/OS. During configuration, job errors might cause unnecessary restarts of the WebSphere Application Server for z/OS address spaces. After installation and configuration, consider enabling ARM.

- If you are ARM-enabled and you cancel or stop a server, it will restart in place using the **armrestart** command.
- It is a good idea to set up an ARM policy for your deployment manager and node agents.
- If you start the location service daemon on a system that already has one, it will terminate.
- Every other server will come up on a dynamic port unless the configuration has a fixed port. Therefore, the fixed ports must be unique in a sysplex.
- If you issue STOP, CANCEL, or MODIFY commands against server instances, be aware of how automatic restart management behaves regarding WebSphere Application Server for z/OS server instances:

Table 543. Behavior of automatic restart management.

This table describes the behavior of automatic restart management regarding WebSphere Application Server for z/OS server instances.

If you issue . . .	ARM will . . .
STOP <i>address_space</i>	not restart the address space
CANCEL <i>address_space</i>	not restart the address space
CANCEL <i>address_space</i> , ARMRESTART	restart the address space
MODIFY <i>address_space</i> , CANCEL	not restart the address space
MODIFY <i>address_space</i> , CANCEL,ARMRESTART	restart the address space

Activating automatic restart management (ARM)

Follow this procedure to activate automatic restart management (ARM).

Before you begin

You must have access to the couple dataset format utility, IXCL1DSU, in SYS1.MIGLIB. If you plan to modify the automatic restart management policy, you must have access to the administrative data utility, IXCMIAPU, also in SYS1.MIGLIB, and have UPDATE authorization to the RACF FACILITY class MVSADMIN.XCF.ARM. To start a policy, you must have READ authorization to the RACF FACILITY class MVSADMIN.XCF.ARM.

About this task

Though servers automatically register with automatic restart management, you must activate the arm component itself, which means you must:

1. Allocate an ARM couple dataset.
2. Start the automatic restart management policy.

If automatic restart management is not active, WebSphere Application Server for z/OS issues an error message to the hardcopy log.

You are not required to change the automatic restart management policy. However, you will have to modify this policy if you want to create custom restart groups. For instance, it is not required or recommended that you start the node agent or deployment manager servers on another system. These servers will never have any transactional recovery to perform. Therefore, they should only be set up for restart-in-place. For complete information about how to modify the policies, see *z/OS MVS Setting Up a Sysplex* (SA22-7625).

The following procedure is intended to give you enough information to get automatic restart management running. Defining automatic restart management policies would require the z/OS manual mentioned above.

Procedure

1. If you have not already formatted a couple dataset for policies, do so now. For details, see *z/OS MVS Setting Up a Sysplex*

2. Submit the job to format the ARM couple dataset.
3. Optional: Modify the automatic restart management policy. To get started, you do not need to modify the policy. If you do want to modify the automatic restart management policy, go to *z/OS MVS Setting Up a Sysplex*, and follow the instructions in that manual.
4. Issue the following operator commands to start the automatic restart management policy:

```
SETXCF COUPLE,TYPE=ARM,PCOUPLE=(dsname,vvvvvv)
SETXCF START,POLICY,TYPE=ARM
```

where

dsname

Is the dataset name for the couple dataset.

vvvvvv

Is the volume serial of the volume on which the couple dataset resides.

Results

You are done when the SETXCF commands complete successfully.

Displaying the status of ARM-registered address spaces:

WebSphere Application Server for the z/OS operating system ships with all control regions issuing Automatic Restart Management (ARM) registration commands. If your installation enables ARM, you can use ARM to display the status of all ARM-registered address spaces, including the address spaces of server instances.

About this task

ARM is used to restart all address spaces that are registered with ARM if they go down. Address spaces that are canceled are not restarted even if they are registered.

Each WebSphere Application Server for z/OS controller registers with ARM. If a controller terminates abnormally or the system fails, ARM will try to restart the failing address spaces. In doing this, ARM will ensure that dependent address spaces are grouped together and will start in the appropriate order. In general, the default ARM policy will restart WebSphere Application Server for z/OS in place. If you are using a sysplex, see “Automatic restart management (ARM)” on page 421 for setup guidelines to ensure that no cross-system restarts are performed.

Perform the following steps to use ARM to display the status of ARM registered address spaces (including the address spaces of server instances):

Procedure

1. Initialize all servers.
2. Display all registered address spaces (including the address spaces of server instances). Issue the following command:

```
d xcf,armstatus,detail
```

Guidelines for changing automatic restart management (ARM) policies

Because server instances register with the default restart group, automatic restart management (ARM) attempts to restart the entire default group on another system in the sysplex when a system failure occurs. To create a restart group other than this default group, you need to follow certain rules.

If you want to create a restart group other than this default group, you need to comply with the following rules and restrictions that apply for z/OS ARM policies. For more information about how to actually change these policies, see, *z/OS MVS Setting Up a Sysplex (SA22-7625)*.

- To change the policy, you need to know the existing element names for the server instances and how to name new elements for additional instances. The element names for these server instances are formed by concatenating the cell short name and the servers specific short name.

If you have a cell named PLEX1 and server named BBOS001, for example, the ARM element name would be PLEX1BBOS001.

Since wildcard characters can be used in the ARM policy, it is possible to exclude an entire group of servers by using a common naming scheme within your cell.

The following section of the ARM policy will prevent any node agents from starting, for example, assuming that each node agent in your cell has a name that adheres to the form BBONxxx:

```
RESTART_GROUP(WEBSPHERE)
ELEMENT(PLEX1BBON*)
RESTART_ATTEMPTS(0,150)
RESTART_TIMEOUT(600)
READY_TIMEOUT(1200)
TERMTYPE(ALLTERM)
RESTART_METHOD(BOTH,PERSIST)
```

This ARM policy will also prevent the node agent from restarting in place. This specification can be modified by changing the RESTART_METHOD and TERMTYPE parameters. See *z/OS MVS Setting Up a Sysplex (SA22-7625)* for more information.

- If you create a restart group, keep the following in the same restart group and set the restart order for the elements as indicated:
 1. RRS
 2. DB2 with IRLM, IMS, CICS, and other transaction or resource managers if used by your application servers in the restart group
 3. Your server instances

Either set up the location service daemon and node agent for restart-in-place or remove them from your ARM policy. Since WebSphere Application Server must be running on all systems that might be used to perform recovery, the application servers will use the location service daemon and node agent that are already running on the alternate system. If the location service daemon attempts to restart on the alternate system, it will fail. If the node agent restarts on the alternate system, it will have no recovery work to do.

Displaying the status of ARM-registered address spaces

WebSphere Application Server for the z/OS operating system ships with all control regions issuing Automatic Restart Management (ARM) registration commands. If your installation enables ARM, you can use ARM to display the status of all ARM-registered address spaces, including the address spaces of server instances.

About this task

ARM is used to restart all address spaces that are registered with ARM if they go down. Address spaces that are canceled are not restarted even if they are registered.

Each WebSphere Application Server for z/OS controller registers with ARM. If a controller terminates abnormally or the system fails, ARM will try to restart the failing address spaces. In doing this, ARM will ensure that dependent address spaces are grouped together and will start in the appropriate order. In general, the default ARM policy will restart WebSphere Application Server for z/OS in place. If you are using a sysplex, see “Automatic restart management (ARM)” on page 421 for setup guidelines to ensure that no cross-system restarts are performed.

Perform the following steps to use ARM to display the status of ARM registered address spaces (including the address spaces of server instances):

Procedure

1. Initialize all servers.

2. Display all registered address spaces (including the address spaces of server instances). Issue the following command:

```
d xcf,armstatus,detail
```

Problem diagnostic plan strategy

Use component trace (CTRACE) to capture and display trace data in trace datasets. Use error log stream to review records that contain error information when WebSphere Application Server for z/OS detects an unexpected condition or failure within its own code. Use BBORBLOG to browse the error log stream.

You can use the following diagnostic tools:

- Component trace
- Error log stream
- Dump datasets

Overview of problem diagnosis

WebSphere Application Server for z/OS uses component trace (CTRACE) to capture and display trace data in trace datasets. WebSphere Application Server for z/OS identifies itself to CTRACE with the short cell name. CTRACE allows you to perform the following tasks:

- Merge multiple traces through the browse tool, including other components such as TCP/IP and z/OS UNIX.
- Write trace data to a dataset rather than to STDOUT, keeping spool space free.
- Better manage system resources by allowing trace data to wrap or not wrap.
- Use CTRACE to funnel trace data from multiple address spaces to one dataset, or have CTRACE send the trace data from each address space to separate datasets.
- Start and stop tracing without stopping and restarting WebSphere Application Server for z/OS address spaces.
- Use one or more datasets for capturing trace data, thus allowing you to manage I/O more effectively.

WebSphere Application Server for z/OS also has an error log stream that records the following error information when WebSphere Application Server for z/OS detects an unexpected condition or failure within its own code:

- Assertion failures
- Unrecoverable error conditions
- Vital resource failures, such as memory
- Operating system exceptions
- Programming defects in WebSphere Application Server for z/OS code

Use the error log stream in conjunction with other facilities available to capture error or status information—such as an activity log, trace data, system logrec, and job log.

The WebSphere Application Server for z/OS error log stream is a system logger application. Because the error log stream uses the system logger, you can perform the following tasks:

- Have error information written to a coupling facility log stream, which provides sysplex-wide error logging, or to a DASD-only log stream, which provides single system-only error logging.

Note: There is a significant performance penalty when using DASD-only error logging.

- Set up either a common log stream for all of WebSphere Application Server for z/OS or individual log streams servers.

Local z/OS client ORBs can also log data in log streams. Because the system logger APIs are unauthorized, any application can use them. You should control access to the log streams through a security product such as RACF.

WebSphere Application Server for z/OS provides a REXX EXEC (BBORBLOG) that allows you to browse the error log stream. By default, the EXEC formats the error records to fit a 3270 display.

Information about using the error log stream to diagnose problems is in the Troubleshooting section of the WebSphere Application Server information center. General information and guidance about the system logger is in *z/OS MVS Setting Up a Sysplex*.

Table 544. Error log stream information.

This table will help you find WebSphere Application Server for z/OS error log stream information.

What is your goal?	You should read:
Learn about the system logger and understand its requirements	<i>z/OS MVS Setting Up a Sysplex</i>
Learn about the WebSphere Application Server for z/OS error log stream	This article
Size the coupling facility structure space needed for the WebSphere Application Server for z/OS error log stream	<i>z/OS MVS Setting Up a Sysplex</i>
Define the WebSphere Application Server for z/OS error log stream	
View the WebSphere Application Server for z/OS error log stream	The Troubleshooting section of the WebSphere Application Server information center
Learn about how Java applications can log messages and trace data in the error log stream	The Applications section of the WebSphere Application Server information center

For details about problem diagnosis, see the Troubleshooting section of the WebSphere Application Server information center.

Planning for component trace

To use CTRACE, perform the following tasks:

- Specify trace options for identifying trace datasets and connecting WebSphere Application Server for z/OS address spaces to the datasets in parmlib members.
- Update WebSphere Application Server for z/OS WebSphere variables to allow for initial trace parameters.
- Use IPCS-CTRACE to view the trace data because you cannot read the trace data in an ordinary editor.

Recommendation for dumps

Plan as you would normally for system dumps. Due to the size of WebSphere Application Server for z/OS address spaces, you might need to resize your system dump datasets and use dynamic dump datasets.

Chapter 9. Configuring the WebSphere Application Server for z/OS product after installation

Use this task to configure WebSphere Application Server for z/OS application serving environments for your z/OS target systems.

Before you begin

- Select a z/OS target system and complete the steps in Chapter 5, “Installing the product on z/OS,” on page 27 and Chapter 7, “Preparing the base z/OS operating system,” on page 67.
- Choose a WebSphere Application Server for z/OS configuration (practice, standalone, or Network Deployment cell) and complete the steps in Chapter 8, “Planning for product configuration on z/OS,” on page 77.

About this task

Configuring a WebSphere Application Server for z/OS application serving environment consists of:

1. Setting up the WebSphere Application Server for z/OS configuration directory for the environment
2. Making any required changes to the z/OS target system that pertain to the particular application serving environment
3. Starting the new environment to verify the configuration

Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a practice standalone application server using the default options then proceed to configure the actual product configuration that you want. See “Building practice WebSphere Application Server for z/OS cells” on page 115 for more information.

WebSphere Application Server for z/OS application serving environment nodes can be created using the workstation-based Profile Management Tool (see “Configuring z/OS application-serving environments with the Profile Management Tool (z/OS only)” or the `zpm` command).

Once a node is configured and running, make further changes using the Web-based administrative console or scripting.

What to do next

Once your application serving environment is up and running, you can install and test applications.

Configuring z/OS application-serving environments with the Profile Management Tool (z/OS only)

You can configure z/OS application serving environments for your z/OS target systems using the Profile Management Tool (z/OS only).

Before you begin

- Choose a z/OS target system, and complete the steps for installing the product and additional software and preparing the base operating system.
- Check that an FTP server is running on the z/OS target system.
- Choose the type of application server environment that you want to configure, and complete the planning steps for that configuration.

About this task

Note: Use the Profile Management Tool (z/OS only) on a workstation running the Windows or Linux Intel operating system to generate the customization definitions for creating profiles and upload the associated jobs and instructions to the target z/OS system.

Configuring a z/OS system application serving environment consists of setting up the application server z/OS environment configuration directory, making required changes to the z/OS target system that pertain to the particular application serving environment, and starting the new environment to verify the configuration. Configuring these application serving environments after product installation requires planning and coordination. If you have not previously configured the application server for z/OS systems, you need to configure a practice standalone application server using the default options. The next step is to configure the product configuration that you want. Read about using the Profile Management Tool (z/OS only), building a practice application server for a z/OS cell and considerations about WebSphere Application Server for z/OS maintenance for more information.

If you have already created a Network Deployment cell, follow the instructions in this article to expand the cell by creating a new federated node or federating an existing standalone application server node into the Network Deployment cell.

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are build with the Profile Management Tool (z/OS only) or the `zpmf` command. After the node is configured and running, make further changes using the administrative console or scripting tool.

After you have installed the z/OS operating system, prepared your z/OS target systems, and planned your new application server environment, perform these tasks to configure and start the application server environment.

Procedure

1. Review the procedures in “Using the Profile Management Tool (z/OS only)” on page 429.
2. Install WebSphere Customization Toolbox.
Read “Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox” on page 44 for more information.
3. Choose the task for the type of application server environment that you want to configure from the following tasks:
 - “Creating standalone application server cells on z/OS using the Profile Management Tool” on page 436
 - “Creating deployment managers on z/OS using the Profile Management Tool” on page 437
 - “Creating Network Deployment cells with application servers on z/OS using the Profile Management Tool” on page 443
 - “Creating managed nodes on z/OS using the Profile Management Tool” on page 440
 - “Federating standalone application servers into Network Deployment cells on z/OS using the Profile Management Tool” on page 442
 - “Creating administrative agents on z/OS using the Profile Management Tool” on page 436
 - “Creating job managers on z/OS using the Profile Management Tool” on page 444
 - “Creating secure proxy administrative agents on z/OS using the Profile Management Tool” on page 445
 - “Creating secure proxy servers on z/OS using the Profile Management Tool” on page 445

What to do next

After your application serving environment is running, you can install and test your applications. You might also want to configure your web servers to interact with your z/OS system.

Tip: If you configured WebSphere Application Server for z/OS using the English Profile Management Tool (z/OS only) and want to allow the display of Japanese characters correctly in your environment, you need to modify some script files.

1. Edit the `setupCmdLine.sh` file
from: `CONSOLE_ENCODING="-Dws.input.encoding=cp1047 -Dws.output.encoding=cp1047"`
to: `CONSOLE_ENCODING="-Dws.input.encoding=cp1399 -Dws.output.encoding=cp1399"`
2. Edit the `wsadmin.sh` file
from: `EXTRA_D_ARGS="-Dfile.encoding=ISO8859-1"`
to: `EXTRA_D_ARGS="-Dfile.encoding=IBM-932"`

Making these two changes will enable you to see the Japanese messages correctly.

Using the Profile Management Tool (z/OS only)

The Profile Management Tool (z/OS only) is a tool, running under the WebSphere Customization Toolbox, that you use for the initial setup of WebSphere Application Server for z/OS cells and nodes.

Before you begin

Install the most current release of the WebSphere Customization Toolbox on a workstation. Read “Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox” on page 44 for more information.

About this task

The Profile Management Tool itself does not create the cells and nodes; instead, it creates batch jobs, scripts, and data files that you can use to perform WebSphere Application Server for z/OS customization tasks. These jobs, scripts, and data files form a customization definition on your workstation that is then uploaded to z/OS and used for customization.

Notes:

- Do not use the Profile Management Tool for WebSphere Application Server Version 6.1, which runs under the Application Server Toolkit, to set up cells and nodes for Version 7.0 and later.
- In WebSphere Application Server for z/OS, you use the Profile Management Tool and the jobs that it generates to create new cells and nodes. After you have created a standalone application server or Network Deployment cell, however, you use the WebSphere Application Server for z/OS administrative console or scripting to administer it.

The Profile Management Tool is intended for use by a systems programmer or WebSphere Application Server for z/OS administrator who is familiar with the z/OS target system on which the resulting WebSphere Application Server for z/OS cells and nodes will run.

The Profile Management Tool uses response files to hold the various values used to create WebSphere Application Server for z/OS customization jobs, scripts and files. These response files remain on the workstation where the Profile Management Tool is run.

- The Profile Management Tool allows you to put these response files on network drives where they can be shared with other users.
- The Profile Management Tool also uploads the associated response file to a DATA member as part of the upload process. This DATA PDS member can then be downloaded to serve as a basis for a new configuration.

Procedure

1. Start the Profile Management Tool.
Read “Starting the Profile Management Tool” on page 430 for more information.

2. Perform any of the following tasks:
 - Create your customization definitions.
Read “Creating customization definitions” on page 431 for more information.
 - Modify the variables in a customization definition, and regenerate the customization jobs associated with it.
 - Delete any existing customization definitions that you want to remove.
 - a. In the WebSphere Application Server for z/OS customization definition table, select the customization definition that you want to delete.
 - b. Click **Delete**.
 - c. Click **Yes**.
 - Review your customization definitions.
Read “Reviewing customization definitions” on page 433 for more information.
 - Upload your customization jobs to a target z/OS system, or export the jobs to the local file system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.

Starting the Profile Management Tool

This article leads you through the tasks involved in starting and using the Profile Management Tool.

Before you begin

Install the most current release of the WebSphere Customization Toolbox on a workstation running the Windows or Linux Intel operating system. Read “Installing, updating, rolling back, and uninstalling the WebSphere Customization Toolbox” on page 44 for more information.

Procedure

1. Open the WebSphere Customization Toolbox.
 - On a Windows operating system, go to **Start > Programs > IBM WebSphere > WebSphere Customization Toolbox *version*** and click **WebSphere Customization Toolbox**.
 - On a Linux operating system, use the menus used to start your programs.
For example, click ***operating_system_menus_to_access_programs > IBM WebSphere > WebSphere Customization Toolbox *version****.
2. If the Profile Management Tool (z/OS only) is not already open, perform the following actions:
 - a. Open the **Welcome** tab, and select **Profile Management Tool (z/OS only)**.
 - b. Read the Welcome information, and then click **Launch Selected Tool**.

What to do next

You can now create or work with a WebSphere Application Server for z/OS customization definition.

Setting Profile Management Tool preferences

You can set Profile Management Tool preferences for the initial setup of WebSphere Application Server for z/OS cells and nodes.

Procedure

1. Start the Profile Management Tool.
Read “Starting the Profile Management Tool” for more information.
2. Click **Window > Preferences > Profile Management Tool**.
3. Select your preferences.

- Select **Enable unique user IDs for daemon and adjunct** to specify that additional user IDs for Websphere Application Server for z/OS processes are to be defined when creating standalone application server, management, and managed nodes.

This option should be selected only if your daemon and control region adjunct processes should run using user IDs that are different from the IDs used to run the associated control region process.

- Select **Enable error log stream and CTRACE parmlib member** to specify that the error log stream name and CTRACE (CTIBBOxx) parmlib member suffix can be defined when creating a Websphere Application Server node.

4. Click **Apply**.

5. Click **OK**.

Creating customization definitions

This article leads you through the tasks involved in creating customization definitions.

Before you begin

Table 545. Worksheets for customization definitions.

Print and complete one of the following worksheets for a customization definition:

Version 8.5	Version 8.0	Version 7.0
"z/OS customization worksheet: Standalone application servers for Version 8.5" on page 151	"z/OS customization worksheet: Standalone application servers for Version 8.0" on page 142	"z/OS customization worksheet: Standalone application servers for Version 7.0" on page 133
"z/OS customization worksheet: Deployment managers for Version 8.5" on page 221	"z/OS customization worksheet: Deployment managers for Version 8.0" on page 214	"z/OS customization worksheet: Deployment managers for Version 7.0" on page 207
"z/OS customization worksheet: Managed (custom) nodes for Version 8.5" on page 256	"z/OS customization worksheet: Managed (custom) nodes for Version 8.0" on page 249	"z/OS customization worksheet: Managed (custom) nodes for Version 7.0" on page 242
"z/OS customization worksheet: Federating application servers for Version 8.5" on page 273	"z/OS customization worksheet: Federating application servers for Version 8.0" on page 271	"z/OS customization worksheet: Federating application servers for Version 7.0" on page 269
"z/OS customization worksheet: Network Deployment cells with application servers for Version 8.5" on page 314	"z/OS customization worksheet: Network Deployment cells with application servers for Version 8.0" on page 304	"z/OS customization worksheet: Network Deployment cells with application servers for Version 7.0" on page 295
"z/OS customization worksheet: Job managers for Version 8.5" on page 351	"z/OS customization worksheet: Job managers for Version 8.0" on page 344	"z/OS customization worksheet: Job managers for Version 7.0" on page 337
"z/OS customization worksheet: Administrative agents for Version 8.5" on page 187	"z/OS customization worksheet: Administrative agents for Version 8.0" on page 180	"z/OS customization worksheet: Administrative agents for Version 7.0" on page 173
"z/OS customization worksheet: Secure proxy servers for Version 8.5" on page 382	"z/OS customization worksheet: Secure proxy servers for Version 8.0" on page 376	"z/OS customization worksheet: Secure proxy servers for Version 7.0" on page 369
"z/OS customization worksheet: Secure proxy administrative agents for Version 8.5" on page 413	"z/OS customization worksheet: Secure proxy administrative agents for Version 8.0" on page 407	"z/OS customization worksheet: Secure proxy administrative agents for Version 7.0" on page 400
Restriction: The worksheets in this column are only applicable to creating Version 8.5 customization definitions.	Restriction: The worksheets in this column are only applicable to creating Version 8.0 customization definitions.	Restriction: The worksheets in this column are only applicable to creating Version 7.0 customization definitions.

About this task

A customization definition consists of a set of files on your workstation that is uploaded to z/OS and used to perform customization tasks.

Use the completed worksheet as a reference when you create your customization definition.

Procedure

1. Start the Profile Management Tool.
Read “Starting the Profile Management Tool” on page 430 for more information.
2. Optional: If you want to add a customization location to the **Customization Locations** table, perform the following actions:
 - a. Click **Add**.
 - b. Select **Add an existing customization location** or **Create a new customization location**.
 - If you are adding an existing customization location, enter the path name of the existing location.
 - If you are creating a new customization location, perform the following tasks:
 - 1) Enter the name that you want to give the location.
 - 2) Select the version of WebSphere Application Server that will be customized by the definitions contained in this location.
 - 3) Enter the path name of the location where you want to store the customization definitions and associated data.
 - c. Click **Finish**.
3. In the **Customization Locations** table, select the location of the customization definition that you want to create.
4. Click the **Customization Definitions** tab if it is not already selected.
5. Click **Create**.
6. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Important: The customization location directory must be empty when you create a new customization location.

Tips:

- Hover your cursor over a field for help information.
- You can also refer to the definitions of the variables in the following articles:
 - “z/OS customization variables: Standalone application servers” on page 118
 - “z/OS customization variables: Deployment managers” on page 194
 - “z/OS customization variables: Managed (custom) nodes” on page 229
 - “z/OS customization variables: Federating application servers” on page 264
 - “z/OS customization variables: Network Deployment cells with application servers” on page 276
 - “z/OS customization variables: Job managers” on page 324
 - “z/OS customization variables: Administrative agents” on page 160
 - “z/OS customization variables: Secure proxy servers” on page 358
 - “z/OS customization variables: Secure proxy administrative agents” on page 389
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

7. Click **Create**.
8. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
- If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.

Reviewing customization definitions

This article explains how to work with a customization definition that you have created in the Profile Management Tool.

Procedure

1. Start the Profile Management Tool.
Read “Starting the Profile Management Tool” on page 430 for more information.
2. In the **Customization Locations** table, select the location of the customization definition that you want to review.
3. In the **Customization Definitions** table, select the customization definition that you want to review.
4. Click the appropriate tabs for information about the customization definition.
 - Click the **Customization Summary** tab for general information about the customization definition.
 - Click the **Customization Instructions** tab for a copy of the customized instructions that were generated when the customization definition was created.
These are the instructions that you use to perform the actual customization after you upload the customization definition to the z/OS target system.

Processing customization definitions using the Profile Management Tool

You can upload the jobs associated with a z/OS customization definition to partitioned datasets on a target z/OS system or export them to a directory on the workstation where the Profile Management Tool is running.

Before you begin

Create the customization definition for the jobs that you want to upload to a target z/OS system or export to the local file system. Read “Creating customization definitions” on page 431 for more information.

Procedure

1. Start the Profile Management Tool.
Read “Starting the Profile Management Tool” on page 430 for more information.
2. In the **Customization Locations** table, select the location of the customization definition that you want to process.
3. In the **Customization Definitions** table, select the customization definition that you want to process.
4. Click **Process**.
5. On the **Select Process Type** panel, select the type of processing that you want to perform on the customization definition.
 - **Upload to target z/OS system using FTP**
Create the customization jobs for the selected customization definition and upload them to a z/OS system using FTP. This option requires an active FTP server on the target z/OS system.

- **Upload to target z/OS system using FTP over SSL**

Create the customization jobs for the selected customization definition and upload them to a z/OS system using FTP over SSL. This option requires an active FTP server on the target z/OS system that is configured to use SSL with TLS authentication.

- **Upload to target z/OS system using secure FTP**

Create the customization jobs for the selected customization definition and upload them to a z/OS system using secure FTP. This option requires an active SSH server on the target z/OS system.

- **Export to local file system**

Create the customization jobs for the selected customization definition and export them to the local file system.

Note: If the customization data have been previously exported to the default directories, the customization jobs in these directories will be uploaded to the target z/OS system when either of the upload options are performed.

6. Click **Next**.

7. Depending on the type of process that you selected, perform one of the following actions:

- On the **Upload Customization Definition Using FTP** panel, specify the necessary upload information.
 - a. In the **Target z/OS system** field, enter the IP name or address of the z/OS system to which you want to upload the customization jobs.
 - b. In the **User ID** field, enter the user ID that you want to use to log on to the FTP server on the target z/OS system.
 - c. In the **Password** field, enter the password for the user ID that you want to use to log on to the FTP server on the target z/OS system.
 - d. In the **FTP server port** field, enter the port number of the FTP server on the target z/OS system.

The default FTP server port number is 21.
 - e. In the **Timeout** field, enter the number of seconds that can elapse without any I/O operation completing before the upload is stopped.

The default timeout value is 20 seconds.
 - f. If you want to allocate the target z/OS datasets, check the box beside **Allocate target z/OS datasets** and complete the two fields that are activated.
 - 1) In the **Volume** field, enter the volume for the target datasets.
 - 2) In the **Unit** field, enter the unit for the target datasets.

Notes:

- The two fields that are activated are optional; but if you specify either field, you must specify the other field as well.
 - If you are uploading the customization jobs to a system different from the system on which you want to run the jobs, you must target a volume that is shared by those systems.
- On the **Upload Customization Definition Using FTP Over SSL** panel, specify the necessary upload information.
 - a. In the **Target z/OS system** field, enter the IP name or address of the z/OS system to which you want to upload the customization jobs.
 - b. In the **User ID** field, enter the user ID that you want to use to log on to the FTP server on the target z/OS system.
 - c. In the **Password** field, enter the password for the user ID that you want to use to log on to the FTP server on the target z/OS system.

- d. In the **FTP server port** field, enter the port number of the FTP server on the target z/OS system.
The default FTP server port number is 21.
- e. In the **Timeout** field, enter the number of seconds that can elapse without any I/O operation completing before the upload is stopped.
The default timeout value is 20 seconds.
- f. If you want to allocate the target z/OS datasets, check the box beside **Allocate target z/OS datasets** and complete the two fields that are activated.
 - 1) In the **Volume** field, enter the volume for the target datasets.
 - 2) In the **Unit** field, enter the unit for the target datasets.

Notes:

- The two fields that are activated are optional; but if you specify either field, you must specify the other field as well.
 - If you are uploading the customization jobs to a system different from the system on which you want to run the jobs, you must target a volume that is shared by those systems.
- On the **Upload Customization Definition Using Secure FTP** panel, specify the necessary upload information.
 - a. In the **Target z/OS system** field, enter the IP name or address of the z/OS system to which you want to upload the customization jobs.
 - b. In the **Target work directory** field, enter the path name of a directory in the UNIX file system on the z/OS system into which the customization data will be uploaded initially.
 - c. In the **User ID** field, enter the user ID that you want to use to log on to the SSH server on the target z/OS system.
 - d. In the **Authentication type** field, select the type of authentication that you want to use to log on to the SSH server on the target z/OS system.
 - e. If you selected **Key** in the **Authentication type** field, enter the pathname of the private key on the local workstation that you want to use to log on to the SSH server on the target z/OS system.
 - f. In the **Password or passphrase** field, enter the password that you use to authenticate with the SSH server if password authorization is selected or the passphrase that you use to protect the private key if key authentication is selected.
 - g. In the **SSH server port** field, enter the port number of the SSH server on the target z/OS system.
The default FTP server port number is 22.
 - h. In the **Timeout** field, enter the number of seconds that can elapse without any I/O operation completing before the upload is stopped.
The default timeout value is 30 seconds.
 - i. If you want to allocate the target z/OS datasets, check the box beside **Allocate target z/OS datasets** and complete the two fields that are activated.
 - 1) In the **Volume** field, enter the volume for the target datasets.
 - 2) In the **Unit** field, enter the unit for the target datasets.

Notes:

- The two fields that are activated are optional; but if you specify either field, you must specify the other field as well.
- If you are uploading the customization jobs to a system different from the system on which you want to run the jobs, you must target a volume that is shared by those systems.

- On the **Export Customization Definition** panel, specify the directory to which you want to export the customization jobs.

Tip: You should not specify an alternate path for the export directories if you might later want to edit any of the generated jobs and then use the upload function to upload the updated jobs to the target z/OS operating system. If you specify an alternate directory, it will be up to you to get the batch jobs to the target z/OS operating system.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** to leave without processing the customization jobs.

8. Click **Finish**.

Creating standalone application server cells on z/OS using the Profile Management Tool

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS standalone application server environment using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for standalone application server cells” on page 117 and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the standalone application server.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Application server** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOSSINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new standalone application server should be running on the z/OS system.

You can now deploy and test applications on your new standalone application server.

Creating administrative agents on z/OS using the Profile Management Tool

You can set up a WebSphere Application Server for z/OS administrative agent using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for an administrative agent and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the administrative agent.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your completed customization worksheet as you proceed through the panels.
Select **Administrative agent** for the server type.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new administrative agent should be running on the z/OS operating system.

What to do next

Register or deregister nodes using the following methods:

- Register a node by issuing the **registerNode** command.
- Deregister a node by issuing the **deregisterNode** command.

Creating deployment managers on z/OS using the Profile Management Tool

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS Network Deployment cell using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for deployment managers” on page 194 and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the deployment manager.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
Select **Deployment manager** for the server type.
2. Review the customization definition to make sure that all of the values are correct.

Read “Reviewing customization definitions” on page 433 for more information.

3. Upload the customization jobs to the target z/OS system.

Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.

4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new deployment managers” for more information.

What to do next

Add application server nodes to your cell using one of two methods:

- Create a new managed node using the Profile Management Tool, and add application servers to it using the administrative console or scripting.
- Federate existing standalone application servers into your Network Deployment cell to create federated nodes with application servers.

Working with your new deployment managers

Once you complete the customization instructions, you will have a WebSphere Application Server for z/OS Network Deployment cell. The Network Deployment cell consists of a deployment manager and a location service daemon. (To run Java EE applications, you must add application server nodes. See below for details.) This article provides useful information for working with your new Network Deployment cell.

Before you begin

Make sure that the WebSphere Application Server for z/OS product HFS and configuration HFS are mounted.

Procedure

1. To start your deployment manager, issue the following MVS console command:

```
START server_proc,JOBNAME=dmgr_name,ENV=cell_name.node_name.dmgr_name
```

where:

- *server_proc* is the deployment manager controller cataloged procedure.
- *dmgr_name* is the deployment manager short name.
- *node_name* is the deployment manager node short name.
- *cell_name* is the cell short name.

If you chose default values, for example, you would enter the following START command:

```
START BB07DCR,JOBNAME=BBODMGR,ENV=BBOCELL.BBODMGR.BBODMGR
```

The START command brings up the deployment manager controller. The controller starts the location service daemon, then uses WLM to start the deployment manager servant. You should see a message similar to the following when the deployment manager is up and running:

```
BB000019I INITIALIZATION COMPLETE FOR WEBSHERE FOR Z/OS CONTROL PROCESS BBODMGR
```

2. Once the deployment manager is successfully started, access the administrative console by pointing a web browser to the following URL:

```
http://hostname:http\_port/ibm/console
```


where:

- *hostname* is the deployment manager HTTP transport host name that you specified during customization.

Note: If you specified * for the deployment manager HTTP host name, this is actually the deployment manager node host name.

- *http_port* is the deployment manager HTTP port that you specified during customization.

Note: The default HTTP port for the deployment manager is 9060.

Until global security is enabled, you will see a signon screen that asks you for a user ID.

The user ID needs to be the one defined during the customization of the dmgr.

You can use the administrative console, scripting, or both to manage the Network Deployment cell and deploy and manage Java EE applications. Before you can deploy applications, however, you need to add application server nodes to your Network Deployment cell.

3. Add an application server node to a Network Deployment cell using one of two methods:
 - Create an (empty) managed node using the Profile Management Tool or **zpm** command. The new node can reside on the same or a different z/OS system as the deployment manager. The new managed node, consisting of just a node agent and perhaps a location service daemon, is federated into the Network Deployment cell. Once this is done, you can use the administrative console or scripting to add application servers and deploy and manage Java EE applications in the node.
See the section *Planning for a new managed node in a Network Deployment cell* in the *Installing your application serving environment* PDF for more information.
 - Federate an existing standalone application server into the Network Deployment cell. The standalone server node becomes a managed node in the Network Deployment cell, along with any Java EE applications that have been deployed on it.
See the section *Planning to federate a standalone server into a Network Deployment cell* in the *Installing your application serving environment* PDF for more information.

Application server nodes (also called managed nodes) in a Network Deployment cell consist of a node agent and any number of application servers per node.

Note: Each z/OS system also needs one location service daemon for each standalone or Network Deployment cell hosted on the system.

4. Use one of the following two methods to stop your deployment manager:
 - Stop the location service daemon, which also stops the deployment manager and any of the cell's managed nodes on the same z/OS system. The location service daemon holds pointers to modules in common storage, and stopping it forces the cell's nodes on the same z/OS system as the location service daemon to shut down. To stop the location service daemon, enter the following MVS console command:

STOP *daemon_jobname*

where *daemon_jobname* is the location service daemon job name. The default location service daemon job name for a Network Deployment cell is BBODMNC.

Note: This is the easiest way to stop the deployment manager.

- Stop just the deployment manager, leaving the location service daemon and any managed nodes on the z/OS system still running. This works because the deployment manager is used to administer only the cell--it does not need to be up for Java EE applications in the cell to run. To stop the deployment manager, enter the following MVS console command:

STOP *dmgr_name*

where *dmgr_name* is the deployment manager short name. The default deployment manager short name is BBODMGR.

Creating managed nodes on z/OS using the Profile Management Tool

This article leads you through the tasks involved in creating a customization definition for a managed server node using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for new managed (custom) nodes” on page 228 and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the managed node.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Managed (custom) node** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOMNINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new managed server nodes” for more information.

Working with your new managed server nodes

Once you complete the customization instructions, you will have a WebSphere Application Server for z/OS application server node (managed node) in your Network Deployment cell.

Before you begin

Make sure that the WebSphere Application Server for z/OS product HFS and configuration HFS are mounted.

Procedure

1. Start your node agent by issuing the following MVS console command:

```
START server_proc,JOBNAME=nodeagent_name,ENV=cell_name.node_name.nodeagent_name
```

where:

- *server_proc* is the node agent cataloged procedure.
- *nodeagent_name* is the node agent short name.
- *node_name* is the node short name.
- *cell_name* is the cell short name.

If you chose default values for example (your sysplex is named CELL1 and your system is named MVSA), you would enter the following START command:

```
START BB07ACR,JOBNAME=BBON001,ENV=CELL1.MVSA.BBON001
```

The START command brings up the node agent. The node agent starts the location service daemon (if one is not already running). You should see a message like the following when the node is up and running:

```
BB000019I INITIALIZATION COMPLETE FOR WEBSHERE FOR z/OS CONTROL PROCESS BBON001
The node agent must be running in order for the deployment manager to administer the node.
```

2. When the deployment manager for the cell is up and running, access the administrative console by pointing a web browser to the following URL:

```
http://hostname:http_port/ibm/console
```

where:

- *hostname* is the deployment manager HTTP transport host name that you specified during customization.

Note: If you specified * for the deployment manager HTTP host name, this is actually the deployment manager node host name.

- *http_port* is the deployment manager HTTP port that you specified during customization.

Note: The default HTTP port for the deployment manager is 9060.

Until administrative security is enabled, you will see a signon screen that asks you for a user ID but no password.

The user ID can be anything and is used only to provide basic tracking of changes. Be aware that until you enable administrative security, anyone with a Web browser and access to the HTTP port can modify your application serving environment.

You can use the administrative console, scripting, or both to manage the node and deploy and manage J2EE applications. Before you can deploy applications, however, you need to add application servers to your managed node.

3. Application servers can be added to the managed server node using the administrative console or scripting. You can use one of the following methods:

- Create a new application server directly using the administrative console or scripting. You can use the controller, servant and CRA cataloged procedures and user IDs created during the managed node setup process for any application servers you create in the managed node. However, after you create additional application servers in an existing node, you must run the following RACF commands:

```
RDEFINE STARTED new_server_short_nameA.* STDATA(USER(controller_region_userid) GROUP(configuration_group))
RDEFINE STARTED new_server_short_nameS.* STDATA(USER(servant_region_userid) GROUP(configuration_group))
```

```
RDEFINE SERVER CB.*.new_cluster_transition_name.* UACC(NONE)
RDEFINE SERVER CB.*.new_cluster_transition_nameADJUNCT.* UACC(NONE)
```

```
PERMIT CB.*.new_cluster_transition_name.* CLASS(SERVER) ID(servant_region_userid) ACC(READ)
```

```
PERMIT CB.*.new_cluster_transition_name.* CLASS(SERVER) ID(controller_region_userid) ACC(READ)
```

```
PERMIT CB.*.new_cluster_transition_nameADJUNCT.* CLASS(SERVER) ID(controller_region_userid) ACC(READ)
```

```
SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH
SETROPTS RACLIST(SERVER) GENERIC(SERVER) REFRESH
```

- Cluster an existing application server in another node, using this managed node as a target. This action creates a cloned copy of the application server being clustered in your new managed node.

4. To start one of your managed node's application servers, issue the following MVS console command:

```
START server_proc,JOBNAME=server_name,ENV=cell_name.node_name.server_name
```

where:

- *server_proc* is the application server agent cataloged procedure (can be the same as the node agent cataloged procedure).
- *nodeagent_name* is the application server short name.
- *node_name* is the node short name.

- *cell_name* is the cell short name.

If you chose the default procedure name for example (your sysplex is named CELL1, your node is named MVSA, and your server is named AZSR01A), you would enter the following START command:

```
START BB07ACR,JOBNAME=AZSR01A,ENV=CELL1.MVSA.AZSR01A
```

The START command brings up the application server controller. The controller starts the location service daemon (if one is not already running) and then uses WLM to start the control region adjunct and the servants. You should see a message similar to the following when the node is up and running:

```
BB000019I INITIALIZATION COMPLETE FOR WEBSPPHERE FOR Z/OS CONTROL PROCESS AZSR01A
```

5. Use one of the following two methods to stop your deployment manager:

- Stop the location service daemon, which also stops any of the cell's nodes on the same z/OS system. The location service daemon holds pointers to modules in common storage, and stopping it forces all cell members on the same z/OS system as the daemon to shut down. To stop the location service daemon, enter the following MVS console command:

```
STOP daemon_jobname
```

where *daemon_jobname* is the location service daemon job name. The default location service daemon job name for a Network Deployment cell is BBODMNC.

- Stop just the node agent and its application servers while leaving the location service daemon, deployment manager (if present), and any other managed nodes on the z/OS system still running. To stop the node agent, enter the following MVS console command:

```
STOP nodeagent_name
```

where *nodeagent_name* is the node agent short name. The default node agent short name is BBON001.

Federating standalone application servers into Network Deployment cells on z/OS using the Profile Management Tool

This article leads you through the tasks involved in federating a WebSphere Application Server for z/OS standalone application server into a Network Deployment cell using the Profile Management Tool.

Procedure

1. Create a customization definition for federating the standalone application server into a Network Deployment cell.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Federate an application server** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct. Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system. Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOANINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new federated application server should be running on the z/OS system. Read “Working with your new federated server nodes” for more information.

Working with your new federated server nodes

After you complete the customization instructions, you have a WebSphere Application Server for z/OS application server federated node.

Procedure

- Check the default host alias list and all other cell-level documents to see if any need to be added in support of the applications and application servers on the newly federated node. Cell-level documents are not automatically updated by the federation process.
- Remove the location service daemon port definitions from your TCP/IP profile for the standalone application server cell because these are not used after federation.

What to do next

Note that web server configurations in an unmanaged node in a standalone application server cell are not migrated as part of federation. Use the administrative console or scripting to add new web server definitions to a Network Deployment cell.

Once these tasks are accomplished, a federated application server node is just like any other application server node. The primary difference is that it already has an application server and applications if they were federated as well. Read “Working with your new managed server nodes” on page 440 for further information.

Creating Network Deployment cells with application servers on z/OS using the Profile Management Tool

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS Network Deployment cell including an initial application server, using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for deployment managers” on page 194 and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the Network Deployment cell.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Cell (deployment manager and an application server)** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.

4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBODMINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new deployment managers” on page 438 for more information.

What to do next

Add application server nodes to your cell using one of two methods:

- Create a new managed node using the Profile Management Tool, and add application servers to it using the administrative console or scripting.
- Federate existing standalone application servers into your Network Deployment cell to create federated nodes with application servers.

Creating job managers on z/OS using the Profile Management Tool

You can set up a WebSphere Application Server for z/OS job manager using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning a job manager and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the job manager.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
Select **Job manager** for the server type.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new job manager should be running on the z/OS operating system.

What to do next

To register application server nodes and deployment managers with the job manager, use the wsadmin **registerWithJobManager** command. The command is in the ManagedNodeAgent command group.

Creating secure proxy servers on z/OS using the Profile Management Tool

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS secure proxy server using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for a secure proxy server and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the secure proxy server.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Secure proxy** under **WebSphere DMZ Secure Proxy Server** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.
Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOSSINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new secure proxy server should be running on the z/OS system.

Creating secure proxy administrative agents on z/OS using the Profile Management Tool

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS administrative agent using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for an administrative agent and Chapter 8, “Planning for product configuration on z/OS,” on page 77.

Procedure

1. Create a customization definition for the administrative agent.
 - a. Follow the instructions in “Creating customization definitions” on page 431.
 - b. Select **Management** under **WebSphere DMZ Secure Proxy Server** for the environment.
 - c. Complete the fields using the values from your customization worksheet as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
Read “Reviewing customization definitions” on page 433 for more information.
3. Upload the customization jobs to the target z/OS system.

Read “Processing customization definitions using the Profile Management Tool” on page 433 for more information.

4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new administrative agent should be running on the z/OS system.

Configuring with symbolic links on z/OS

Symbolic links can be used in configuring and maintenance for WebSphere Application Server for z/OS applications.

About this task

When a WebSphere Application Server for z/OS node is built, the configuration HFS is peppered with hundreds of symbolic links. These symbolic links point to files in the product HFS supplied by IBM. There is good reason for having this design. Unfortunately, if you configure two or more nodes that point directly to the mount point of the product HFS, then applying maintenance to the product HFS necessarily means updating all the nodes at once.

The way to provide flexibility is to configure what is known as an **intermediate symbolic link** between the node's configuration HFS and the actual mount point of the product HFS. The result is two symbolic links: the configuration HFS link pointing to the intermediate link, and the intermediate link then pointing to the product HFS. The value of this is that a node can point to a new level of the product HFS by simply changing the one intermediate symbolic link.

What to do next

Read <http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100396> for additional information on the use of **intermediate symbolic links**.

Configuring z/OS application-serving environments with the `zpm` command

You can configure WebSphere Application Server for z/OS application-serving environments for your z/OS target systems using the `zpm` command. The `zpm` command creates the same batch jobs and data files as the workstation-based Profile Management Tool, but the command runs under z/OS rather than on a workstation.

Before you begin

- Choose a z/OS target system and complete the steps in Chapter 5, “Installing the product on z/OS,” on page 27 and Chapter 7, “Preparing the base z/OS operating system,” on page 67.
- Choose the type of application server environment that you want to configure, and complete the planning steps for that configuration.

About this task

The `zpm` command is an alternative to the workstation-based Profile Management Tool, which is launched from the WebSphere Customization Toolbox. You can use this command if you do not have a Windows or

Linux workstation available to run the WebSphere Customization Toolbox or if you need to automate the generation of the WebSphere for z/OS customization jobs. You launch this command on the z/OS system that you need to configure using a shell script.

Configuring a WebSphere Application Server for z/OS application serving environment consists of setting up the WebSphere Application Server for z/OS configuration directory for the environment, making any required changes to the z/OS target system that pertain to the particular application serving environment, and starting the new environment to verify the configuration. Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a practice standalone application server using the sample response file. Then proceed to configure the actual product configuration that you want. See the sample files below for more information.

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are build with the Profile Management Tool or the **zpm**t command. After the node is configured and running, make further changes using the administrative console or scripting tool.

After you have installed the WebSphere Application Server for z/OS product, prepared your z/OS target systems, and planned your WebSphere Application Server for z/OS environment, perform the tasks in this section to configure needed response files.

Procedure

1. Follow the directions for the type of response file that you want to configure. If you have already prepared a response file, proceed to the next step.
 - For a standalone application server, refer to the list of variables and definitions in “Variables for configuring standalone application servers using the zpm
 - For a deployment manager, refer to the list of variables and definitions in “Variables for configuring deployment managers using the zpm
 - For a managed (custom) node, refer to the list of variables and definitions in “Variables for configuring managed (custom) nodes using the zpm
 - For a federated node, refer to the list of variables and definitions in “Variables for federating application servers using the zpm
 - For a Network Deployment cell with an application server, refer to the list of variables and definitions in “Variables for configuring Network Deployment cells with application servers using the zpm
 - For an administrative agent, refer to the list of variables and definitions in “Variables for configuring administrative agents using the zpm
 - For a job manager, refer to the list of variables and definitions in “Variables for configuring job managers using the zpm
 - For a secure proxy server, refer to the list of variables and definitions in “Variables for configuring secure proxy servers using the zpm
 - For a secure proxy administrative agent, refer to the list of variables and definitions in “Variables for configuring secure proxy administrative agents using the zpm

2. On your target z/OS system, run the `zpmt.sh` shell script using your prepared response file. This tool will create the `.CNTL` and `.DATA` files needed to run the required jobs. The response file needs to be located in the UNIX (USS) file system. For command syntax, refer to the `zpmt.sh` shell script file: “`zpmt` command.”
3. Follow the instructions in the `xxxxxINS` member of the `.CNTL` data to create the application serving environment.

What to do next

When your application serving environment is running, you can install and test your applications. You might also want to configure your web servers to interact with WebSphere Application Server for z/OS.

Tip: If you configured WebSphere Application Server for z/OS using the English `zpmt` command and want to allow the display of Japanese characters correctly in your environment, you need to modify some script files.

1. Edit the `setupCmdLine.sh` file
from: `CONSOLE_ENCODING="-Dws.input.encoding=cp1047 -Dws.output.encoding=cp1047"`
to: `CONSOLE_ENCODING="-Dws.input.encoding=cp1399 -Dws.output.encoding=cp1399"`
2. Edit the `wsadmin.sh` file
from: `EXTRA_D_ARGS="-Dfile.encoding=ISO8859-1"`
to: `EXTRA_D_ARGS="-Dfile.encoding=IBM-932"`

Making these two changes will enable you to see the Japanese messages correctly.

zpmt command

The `zpmt` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring the WebSphere Application Server for z/OS product.

Location of the shell script

The `zpmt.sh` shell script is located in the `smpe_install_root/bin` or `was_home/bin` directory.

Description of the shell script syntax

-responseFile

Specifies the path to your response file

-profilePath

Specifies a fully qualified path name to an existing set of generated jobs

This parameter cannot be used in combination with the `-responsefile` option.

-workspace

Specifies the Eclipse workspace directory

-transfer

Copies generated jobs from a UNIX System Services (USS) file system to a pair of partitioned datasets

The `zpmt` command first writes the customization jobs to a USS file system.

-replace

Specifies that if a set of jobs for the specified `profilePath` already exist, they are to be overwritten

This parameter cannot be used without both the `-workspace` and `-responseFile` arguments.

-allocate

Attempts to allocate the target datasets

This parameter cannot be used without the `-transfer` option.

-installExtension

Installs a feature-pack or stacked-product extension

This must include the absolute path name of the SMP/E installation root for a stacked product or feature pack. Using this parameter extracts the contents of the WebSphere Configuration Tool archive file contained within the specified installation file system and installs its contents into the Eclipse workspace directory

-listExtensions

Lists the extensions that are currently installed in the specified Eclipse workspace directory

-uninstallExtension

Removes the specified extension from the specified Eclipse workspace directory

-version

Version number of the extension to uninstall

Use this parameter to uninstall a specific version of an extension.

Datasets are determined by appending the values `.CNTL` and `.DATA` to the `zTargetHLQ` value for the profile containing the jobs that are being copied. This operation overwrites existing files of the same name in those datasets.

Sample syntax

The following examples describe typical command lines with attributes for the `zpmt` command. In these examples, `/xxx` can be any directory to which the user invoking `zpmt.sh` has read and write access.

- `zpmt.sh -workspace /xxx -transfer -allocate -responseFile /xxx/ZCellcmd.responseFile`

This does the following:

- Generates the customization jobs to the location specified by `profilePath` in the response file
- Allocates the target `CNTL` and `DATA` datasets using the high-level qualifier specified by `targetHLQ` in the response file
- Transfers the jobs from the file system to the `CNTL` and `DATA` datasets

- `zpmt.sh -workspace /xxx -responseFile /xxx/ZAppSrvcmd.responseFile`

This generates the customization jobs to the location specified by `profilePath` in the response file.

- `zpmt.sh -workspace /xxx -allocate -transfer -profilePath /xxx/ZAppSrvcmd`

This does the following:

- Allocates the target `CNTL` and `DATA` datasets using the high-level qualifier specified by `targetHLQ` in the response file
- Transfers the generated jobs at the location specified by `-profilePath` to those datasets

Note: This usage assumes the jobs have already been generated with a previous invocation of `zpmt.sh`.

- `zpmt.sh -workspace /xxx -transfer -responseFile /xxx/ZDmgrcmd.responseFile`

This transfers the generated jobs from location `profilePath` in the response file to the generated `CNTL` and `DATA` datasets.

Note: This usage assumes that the jobs have already been generated with a previous invocation of `zpmt.sh` and that the target `CNTL` and `DATA` datasets have already been allocated

- `zpmt.sh -workspace eclipse_workspace_dir -responseFile response_file -allocate -transfer -replace -installExtension stacked_product_or_feature_pack_install_root`

This does the following:

- Installs the extension from the specified stack-product or feature-pack installation image

- Generates the customization jobs to the location specified by profilePath in the response file (any existing customization jobs at this location are replaced)
- Allocates the target CNTL and DATA datasets using the high-level qualifier specified by targetHLQ in the response file
- Transfers the generated jobs from the file system to the CNTL and DATA datasets
- `zpmt.sh -workspace eclipse_workspace_dir -listExtensions`
This generates a list of the extensions that are currently installed in the specified Eclipse workspace directory.
- `zpmt.sh -workspace eclipse_workspace_dir -uninstallExtension extension_name -version extension_version`
This removes the specified version of the specified extension from the specified Eclipse workspace directory.

Variables for configuring standalone application servers using the zpmt command

The `zpmt` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a standalone application server.

Tip: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Action

create Action to be taken

Profile information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Performance tuning setting (applyPerfTuningSetting)

Performance-tuning setting that most closely matches the type of environment in which the application server will run

standard

The standard settings are optimized for general-purpose usage.

production

The production performance settings are appropriate for a production environment where application changes are rare and optimal runtime performance is important.

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration.

The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is ZFS.

Product file system information customization

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a Network Deployment cell, ensure that the standalone server cell name is different from the Network Deployment cell name.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Install administrative console? (zInstallAdminConsole)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS administrative console.

Note: These applications are not supported in a Network Deployment cell.

Install default application? (zInstallDefaultApp)

Specify whether you do (true) or do not (false) want to deploy the default WebSphere Application Server for z/OS application.

Server address space information customization

Rule: In the following, unless specified otherwise, names must be eight or fewer characters.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the application server controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the application server controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the application server servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the application server servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Control region adjunct information

Procedure name (zAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zAdjunctUserid)

User ID associated with application server control region adjuncts in the node

UID (zAdjunctUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Server TCP/IP information customization

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zOrbListenerPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zOrbListenerSslPort)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

HTTP transport port (zHttpTransportPort)

Port for HTTP requests

Rule: Value cannot be 0.

HTTPS transport port (zHttpTransportSslPort)

Port for secure HTTP requests

Rule: Value cannot be 0.

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

Service integration port (zServiceIntegrationPort)

Port for service-integration requests

Rule: Value cannot be 0.

Service integration secure port (zServiceIntegrationSecurePort)

Port for secure service-integration requests

Rule: Value cannot be 0.

Service integration MQ interoperability port (zServiceIntegrationMqPort)

Port for service-integration MQ interoperability requests

Rule: Value cannot be 0.

Service integration MQ interoperability secure port (zServiceIntegrationSecureMqPort)

Port for secure service-integration MQ interoperability requests

Rule: Value cannot be 0.

Session initiation protocol (SIP) port (zSessionInitiationPort)

Port for session initiation requests

Rule: Value cannot be 0.

Session initiation protocol secure port (zSessionInitiationSecurePort)

Port for secure session initiation requests

Rule: Value cannot be 0.

Administration overlay UDP port (zAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions

Administration overlay TCP port (zAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is `*`.

Rule: The default is `*` or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select `true` to register your location service daemon with it. Otherwise, select `false`.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select `true` to generate a new CA certificate. Select `false` to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected `false` for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select `true` if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select `true` if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify `true`, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (`adminUserName`)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (`adminPassword`)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (`personalCertDN`)

Identifier of the personal certificate

Issued by distinguished name (`signingCertDN`)

Identifier of the root signing certificate

Expiration period in years (`personalCertValidityPeriod`)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (`signingCertValidityPeriod`)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (`keyStorePassword`)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Web server customization

Note:

Only one web server can be defined on a standalone application server.

Create a web server definition (`webServerCheck`)

Web server type (`webServerType`)

Valid values: IHS, HTTPSERVER_ZOS, APACHE, IPLANET, DOMINO, IIS

Web server operating system (`webServerOS`)

Valid values: Windows, Linux, Solaris, AIX, HPUX, OS390, OS400

Web server name (`webServerName`)

Name used in defining the web server in the administrative console

Web server host or IP address (`webServerHostname`)

IP name or address of the z/OS system on which the web server is located

Web server port (`webServerPort`)

HTTP Port on which the web server is listening

Web server install directory path (webServerInstallPath)

Varies by user configuration

Web server plugin install directory path (webServerPluginPath)

Varies by user configuration

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for configuring deployment managers using the zpmt command

The **zpmt** command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a deployment manager.

Tip: See the sample response file in the *app_server_root/zOS-config/zpmt/samples* directory.

Recommendation: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Action

create Action to be taken

Server type

Server type (serverType)

Type of server to be created within this management profile

Profile information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as *config_hlq*) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are

configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

gotcha: If you run the RACF job in the Profile Management Tool, the controller ID, the servant ID, and the administrator ID are automatically added to the configuration group. If you do not run the RACF job in the Profile Management Tool, you must explicitly add these IDs to the configuration group for the deployment manager to enable the controller to remove temporary directories and files that the servant creates.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is ZFS.

Product file system information customization

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: The deployment manager is not clusterable, so this value never actually becomes the cluster short name of this server's cluster. However, like an application server, the deployment manager still needs an APPLENV, so the cluster transition name is used for this purpose.

Rule: Name must be eight or fewer characters and all uppercase.

Server address space information customization

Rule: In the following, unless specified otherwise, names must be eight or fewer characters.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server TCP/IP information customization

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port (zCellDiscoveryPort)

Port number used by node agents to connect to this deployment manager server.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zOrbListenerPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zOrbListenerSslPort)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port (zDataPowerManagementPort)

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager

Middleware agent RPC port (zMiddlewareAgentPort)

Communications port for WebSphere Extended Deployment administrative functions

The default is 7060.

Administration overlay UDP port (zAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions

The default is 11005.

Administration overlay TCP port (zAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions

The default is 11006.

Status update listener port (zStatusListenerPort)

Port that job managers and deployment managers listen on for status updates coming from registered nodes

The default is 9420.

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select true if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID.

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (personalCertDN)

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for configuring managed (custom) nodes using the zpmt command

The **zpmt** command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a managed (custom) node.

Tip: See the sample response file in the *app_server_root/zOS-config/zpmt/samples* directory.

Recommendation: Use the IBM default names the first time that you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Action

create Action to be taken

Profile information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as *config_hlq*) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 300 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is ZFS.

Product file system information customization**Product file system directory (zSmpePath)**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short node name (zNodeShortName)**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server address space information customization

Rule: In the following, names must be eight or fewer characters unless specified otherwise.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Control region adjunct information

Procedure name (zAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zAdjunctUserid)

User ID associated with application server control region adjuncts in the node

UID (zAdjunctUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Node TCP/IP information customization

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Target deployment manager does not reside in same sysplex (zInterPlexManagedNode)

If your target deployment manager does not reside in same sysplex, select true and specify the following parameters. Otherwise, select false.

IP Name (zDaemonIPName)

The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

Notes:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization.

Listen IP (zDaemonListenIP)

Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want; but once chosen, it is difficult to change, even in the middle of customization.

SSL port (zDaemonSslPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select true if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on

z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Federation information

Node host name or IP address (zFederateDmaNodeHostname)

TCP/IP node name of the deployment manager for the Network Deployment cell

Deployment manager JMX connection type (zFederateDmaPortType)

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port (zFederateDmaPort)

JMX (Java Management Extensions) SOAP (Simple Object Access Protocol) connector port that the add-node request uses to connect to the deployment manager

It provides the federation process with knowledge of which deployment manager is the target of the federation.

Deployment manager security is enabled (zFederateDmaSecurity)

Specify true if administrative security is enabled on the Network Deployment cell and the deployment manager.

User ID (zFederateDmaSecurityUserID)

User ID with full administrative privileges for the Network Deployment cell

This is the security domain administrator user ID and cannot be changed.

Password (zFederateDmaSecurityPassword)

Password for user ID

Node group name (zNodeGroupName)

Node group into which the node will be placed.

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

ORB listener IP name (zFederateOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zFederateOrbPortName)

Port for IIOp requests that acts as the bootstrap port for the server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zFederateOrbSslPortName)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

Short node agent server name (zFederateServerShortName)

Name of the node agent server

This is the server's job name, as specified in the MVS START command JOBNAME parameter. This value identifies the server to z/OS facilities such as SAF.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long node agent server name (zFederateServerName)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console . The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port (zFederateJmxSoapConnectorPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

Node discovery port (zFederateNodeDiscoveryPort)

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager

Node multicast discovery port (zFederateNodeMulticastDiscoveryPort)

Defines the multicast port through which the node agent sends discovery requests to its managed servers

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port (zFederateNodeIPv6MulticastDiscoveryPort)

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port (zFederateAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zFederateHamCommPort)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node middleware agent RPC port (zMiddlewareAgentPort)

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port (zAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port (zAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Launch the node agent after node federation (zFederateNodeAgentAfterFederation)

Specify true if you want the node agent to be started automatically after federating a node. Otherwise, specify false.

Security certificate customization

Default personal certificate

Issued to distinguished name (personalCertDN)

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for federating application servers using the zpmt command

The `zpmt` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for federating an application server.

Tip: See the sample response file in the `app_server_root/zOS-config/zpmt/samples` directory.

Action

create Action to be taken

Federation information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as `config_hlq`) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configuration group name (zConfigurationGroup)

Group name of the WebSphere Application Server configuration group

Configuration user ID (zAdminUserid)

User ID that owns the configuration file system

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Node host name or IP address (zFederateDmaNodeHostname)

TCP/IP node name of the deployment manager for the Network Deployment cell

Deployment manager JMX connection type (zFederateDmaPortType)

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port (zFederateDmaPort)

JMX (Java Management Extensions) SOAP (Simple Object Access Protocol) connector port that the add-node request uses to connect to the deployment manager

It provides the federation process with knowledge of which deployment manager is the target of the federation.

Deployment manager security is enabled (zFederateDmaSecurity)

Specify true if administrative security is enabled on the Network Deployment cell and the deployment manager.

User ID (zFederateDmaSecurityUserID)

User ID with full administrative privileges for the Network Deployment cell

This is the security domain administrator user ID and cannot be changed.

Password (zFederateDmaSecurityPassword)

Password for user ID

Application Server security enabled (zFederateAppServerSecurity)

This is required if global security is enabled on the cell containing the node that is being federated.

User ID (zFederateAppServerSecurityUserID)

User ID with full administrative privileges for the cell containing the application server

Password (zFederateAppServerSecurityPassword)

Password for user ID

Include applications? (zFederateIncludeApps)

Specify true if you want to include applications with your deployment manager node. Enabling this option instructs the addNode program to include applications from the node, as it would remove them prior to federation otherwise. If the application already exists in the cell, a warning is printed and the application is not installed into the cell.

Note: You must use this option to migrate all the applications to the new cell. Federating the node to a cell using the addNode command does not merge any cell-level configuration information, including that from virtualHost.

Node group name (zNodeGroupName)

Node group into which the node will be placed.

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

ORB listener IP name (zFederateOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zFederateOrbPortName)

Port for IIOp requests that acts as the bootstrap port for the server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zFederateOrbSslPortName)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

Short node agent server name (zFederateServerShortName)

Name of the node agent server

This is the server's job name, as specified in the MVS START command JOBNAME parameter. This value identifies the server to z/OS facilities such as SAF.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long node agent server name (zFederateServerName)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console. The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port (zFederateJmxSoapConnectorPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

Node discovery port (zFederateNodeDiscoveryPort)

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager

Node multicast discovery port (zFederateNodeMulticastDiscoveryPort)

Defines the multicast port through which the node agent sends discovery requests to its managed servers

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port (zFederateNodeIPv6MulticastDiscoveryPort)

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port (zFederateAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zFederateHamCommPort)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node middleware agent RPC port (zMiddlewareAgentPort)

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port (zAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port (zAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Launch the node agent after node federation (zFederateNodeAgentAfterFederation)

Specify `true` if you want the node agent to be started automatically after federating a node. Otherwise, specify `false`.

Application server ORB listener port (zFederateAppServerOrbPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

Note: The add node operation creates the node agent administrative server with a default ORB listener port equivalent to the INS CosNaming default bootstrap port. Because this same port was previously used by the node's initial standalone server, the initial standalone server's ORB listener port must change to a new port value. The default value to which the application server's ORB listener port is set is 9810. If you configure multiple cells that intersect the same systems, use of the default value will cause a port conflict between these cells. This option helps you set the port number in case port 9810 was previously assigned.

Federate service integration busses that exist on this node? (zFederateFederateSib)

Specify `true` to federate service integration busses that exist on this node. Otherwise, specify `false`.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for configuring Network Deployment cells with application servers using the zpmt command

The `zpmt` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a Network Deployment cell with an application server.

Tip: See the sample response file in the `app_server_root/zOS-config/zpmt/samples` directory.

Action

create Action to be taken

Profile information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as `config_hlq`) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Deployment manager configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is ZFS.

Application server configuration file system customization

Mount point (zAppServerConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zAppServerConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zAppServerWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zAppServerConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zAppServerConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zAppServerConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zAppServerFilesystemType)

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

The default is ZFS.

Deployment manager system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Application server file system information

Product file system directory (zAppServerSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zAppServerEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

Intermediate symbolic link (zAppServerIntermediateSymlink)

The default value for zAppServerIntermediateSymlink is the zAppServerConfigMountPoint value appended by /wasInstall.

Deployment manager server customization

Short cell name (zCellShortName)

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: The deployment manager is not clusterable, so this value never actually becomes the cluster short name of this server's cluster. However, like an application server, the deployment manager still needs an APPLENV, so the cluster transition name is used for this purpose.

Rule: Name must be eight or fewer characters and all uppercase.

Application server customization**Short node name (zAppServerNodeShortName)**

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Short server name (zAppServerServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (zAppServerServerName)

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Long node name (appServerNodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Cluster transition name (zAppServerClusterTransitionName)

WLM APPL ENV (WLM application environment) name for this server

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Install administrative console? (zInstallAdminConsole)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS administrative console.

Note: These applications are not supported in a Network Deployment cell.

Install default application? (zInstallDefaultApp)

Specify whether you do (true) or do not (false) want to deploy the default WebSphere Application Server for z/OS application.

Server address space information customization

Rule: In the following, names must be eight or fewer characters unless specified otherwise.

Deployment manager controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Deployment manager servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Application server controller information

Procedure name (zAppServerControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

Application server servant information

Procedure name (zAppServerServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

Application server controller adjunct information

Procedure name (zAppServerAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

Deployment manager TCP/IP information

Note: Do not choose port values that are already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port (zCellDiscoveryPort)

Port number used by node agents to connect to this deployment manager server.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zOrbListenerPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zOrbListenerSslPort)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port (zDataPowerManagementPort)

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager

Middleware agent RPC port (zMiddlewareAgentPort)

Communications port for WebSphere Extended Deployment administrative functions (XDAGENT_PORT)

The default is 7060.

Administration overlay UDP port (zAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_UDP_LISTENER_ADDRESS)

The default is 11005.

Administration overlay TCP port (zAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions (OVERLAY_TCP_LISTENER_ADDRESS)

The default is 11006.

Status update listener port (zStatusListenerPort)

Port that job managers and deployment managers listen on for status updates coming from registered nodes (STATUS_LISTENER_ADDRESS)

The default is 9420.

Application server TCP/IP information

Note: Do not choose port values already in use.

SOAP JMX Connector port (zAppServerSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB listener port (zAppServerOrbListenerPort)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port (zAppServerOrbListenerSslPort)

Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport port (zAppServerHttpTransportPort)

Port for HTTP requests (WC_defaulthost)

Rule: Value cannot be 0.

HTTPS transport port (zAppServerHttpTransportSslPort)

Port for secure HTTP requests (WC_defaulthost_secure)

Rule: Value cannot be 0.

Administrative interprocess communication port (zAppServerAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zAppServerHighAvailManagerPort)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

Service integration port (zAppServerServiceIntegrationPort)

Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration secure port (zAppServerServiceIntegrationSecurePort)

Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability port (zAppServerServiceIntegrationMqPort)

Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration MQ interoperability secure port (zAppServerServiceIntegrationSecureMqPort)

Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Session initiation protocol (SIP) port (zAppServerSessionInitiationPort)

Port for session initiation requests (SIP_DEFAULTHOST)

Rule: Value cannot be 0.

Session initiation protocol secure port (zAppServerSessionInitiationSecurePort)

Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Rule: Value cannot be 0.

Administration overlay UDP port (zAppServerAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions (zAppServer_OVERLAY_UDP_LISTENER_ADDRESS)

Administration overlay TCP port (zAppServerAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions (zAppServer_OVERLAY_TCP_LISTENER_ADDRESS)

Node agent TCP/IP information**ORB listener port (zNodeAgentOrbPortName)**

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL listener port (zNodeAgentOrbSslPortName)

Port for secure IIOp requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

Short node agent server name (zNodeAgentServerShortName)

Name of the node agent server

This is the server's job name, as specified in the MVS START command JOBNAME parameter. This value identifies the server to z/OS facilities such as SAF.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long node agent server name (zNodeAgentServerName)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console . The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port (zNodeAgentJmxSoapConnectorPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

Node discovery port (zNodeAgentNodeDiscoveryPort)

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager

Node multicast discovery port (zNodeAgentNodeMulticastDiscoveryPort)

Defines the multicast port through which the node agent sends discovery requests to its managed servers

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port (zNodeAgentNodeIPv6MulticastDiscoveryPort)

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port (zNodeAgentAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zNodeAgentHamCommPort)

Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node middleware agent RPC port (zNodeAgentMiddlewareAgentPort)

Communications port for WebSphere Extended Deployment administrative functions (NODE_XDAGENT_PORT)

Node administration overlay UDP port (zNodeAgentAdminOverlayUDPPort)

UDP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_UDP_LISTENER_ADDRESS)

Node administration overlay TCP port (zNodeAgentAdminOverlayTCPPort)

TCP communications port for WebSphere Extended Deployment administrative functions (NODE_OVERLAY_TCP_LISTENER_ADDRESS)

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select `true` to register your location service daemon with it. Otherwise, select `false`.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select `true` to generate a new CA certificate. Select `false` to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected `false` for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select `true` if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select `true` if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify `true`, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (`zSecurityDomainId`)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (`zSAFProfilePrefix`)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (`zAdminUserId`)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (`zAdminUid`)

Valid UID for this user ID

Unauthenticated User ID (`zAdminUnauthenticatedUserId`)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (`zAdminUnauthenticatedUid`)

Valid UID for this user ID

Enable writable SAF keyring support (`zEnableWritableKeyring`)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (`adminUserName`)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (`adminPassword`)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (`personalCertDN`)

Identifier of the personal certificate

Issued by distinguished name (`signingCertDN`)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years (signingCertValidityPeriod)**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Web server customization**Create a web server definition (webServerCheck)****Web server type (webServerType)**

Valid values: IHS, HTTPSERVER_ZOS, APACHE, IPLANET, DOMINO, IIS

Web server operating system (webServerOS)

Valid values: Windows, Linux, Solaris, AIX, HPUX, OS390, OS400

Web server name (webServerName)

Name used in defining the web server in the administrative console

Web server host or IP address (webServerHostname)

IP name or address of the z/OS system on which the web server is located

Web server port (webServerPort)

HTTP Port on which the web server is listening

Web server install directory path (webServerInstallPath)

Varies by user configuration

Web server plugin install directory path (webServerPluginPath)

Varies by user configuration

Job statement customization**Job statement 1 (zJobStatement1)****Job statement 2 (zJobStatement2)****Job statement 3 (zJobStatement3)****Job statement 4 (zJobStatement4)****Variables for configuring administrative agents using the zpmt command**

The **zpmt** command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring an administrative agent.

Tip: See the sample response file in the *app_server_root/zOS-config/zpmt/samples* directory.

Server type**Server type (serverType)**

Type of server to be created within this management profile

Profile information**Profile name (profileName)**

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information**Target operating system (targetOS)**

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration**Configuration group (zConfigurationGroup)****Allow OS security to assign GID (zConfigurationGroupGID)**

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)**Allow OS security to assign GID (zLocalUserGroupGID)**

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations**System name (zSystemName)**

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMB0LS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization**Mount point (zConfigMountPoint)**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See "Product file system" on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

System information**Product file system directory (zSmpePath)**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server address space information customization

In the following, names must be eight or fewer characters unless specified otherwise.

Controller information**Procedure name (zControlProcName)**

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information**Procedure name (zServantProcName)**

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zOrbListenerPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zOrbListenerSslPort)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select `true` to register your location service daemon with it. Otherwise, select `false`.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select `true` to generate a new CA certificate. Select `false` to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected `false` for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select `true` if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select `true` if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify `true`, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

Administrator user ID (zAdminUserId)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

Unauthenticated User ID (zAdminUnauthenticatedUserId)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization**Default personal certificate****Issued to distinguished name (personalCertDN)**

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years (signingCertValidityPeriod)**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization**Job statement 1 (zJobStatement1)****Job statement 2 (zJobStatement2)****Job statement 3 (zJobStatement3)****Job statement 4 (zJobStatement4)****Variables for configuring job managers using the zpmt command**

The `zpmt` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a job manager.

Tip: See the sample response file in the `app_server_root/zOS-config/zpmt/samples` directory.

Server type**Server type (serverType)**

Type of server to be created within this management profile

Profile information**Profile name (profileName)**

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information**Target operating system (targetOS)**

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as `config_hlq`) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are

configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

System information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server address space information customization

In the following, names must be eight or fewer characters unless specified otherwise.

Controller information**Procedure name (zControlProcName)**

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information**Procedure name (zServantProcName)**

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOp requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB listener port (zOrbListenerPort)

Port for IIOp requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOp requests

Rule: Value cannot be 0.

ORB SSL listener port (zOrbListenerSslPort)

Port for secure IIOp requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Status update listener port (zStatusListenerPort)

Port that job managers and deployment managers listen on for status updates coming from registered nodes

The default is 9425.

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOp IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select true if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (**zSecurityDomainId**)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

Administrator user ID (**zAdminUserid**)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (**zAdminUid**)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (**zAdminUnauthenticatedUserid**)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (**zAdminUnauthenticatedUid**)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (**zEnableWritableKeyring**)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (**adminUserName**)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (**adminPassword**)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (**personalCertDN**)

Identifier of the personal certificate

Issued by distinguished name (**signingCertDN**)

Identifier of the root signing certificate

Expiration period in years (**personalCertValidityPeriod**)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization**Job statement 1 (zJobStatement1)****Job statement 2 (zJobStatement2)****Job statement 3 (zJobStatement3)****Job statement 4 (zJobStatement4)****Variables for configuring secure proxy servers using the zpmt command**

The **zpmt** command uses the values that you specify in for the variables defined in a response file to create customization data and instructions for configuring a secure proxy server.

Tip: See the sample response file in the *app_server_root/zOS-config/zpmt/samples* directory.

Profile information**Profile name (profileName)**

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information**Target operating system (targetOS)**

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as *config_hlq*) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMB0LS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

Product file system information customization**Product file system directory (zSmpePath)**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a Network Deployment cell, ensure that the standalone server cell name is different from the Network Deployment cell name.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rules: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster. See “z/OS JCL cataloged procedures” on page 82 for more information.

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Security level information

Proxy security level (securityLevel)

High Represents the highest level of proxy server security based on certain proxy server settings

Medium Represents the mid-level of proxy server security based on certain proxy server settings

Low Represents the lowest level of proxy server security based on certain proxy server settings

Supported protocols (supportedProtocols)

Web Select to support web protocol

SIP Select to support SIP protocol

Server address space information customization

In the following, names must be eight or fewer characters unless specified otherwise.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the application server controller

Rules: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the application server controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Server TCP/IP information customization

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

Bootstrap port (zBootstrapPort)

Port for IIOp requests that acts as the bootstrap port for this server

Rule: Value cannot be 0.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's web container should listen for incoming HTTP requests

The default is *, which instructs the web container to listen on all available IP addresses.

Note: The transport host name becomes the hostname in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

HTTP transport port (zHttpTransportPort)

Port for HTTP requests

Rule: Value cannot be 0.

HTTPS transport port (zHttptransportSslPort)

Port for secure HTTP requests

Rule: Value cannot be 0.

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Session initiation protocol (SIP) port (zSessionInitiationPort)

Port for session initiation requests

Rule: Value cannot be 0.

Session initiation protocol secure port (zSessionInitiationSecurePort)

Port for secure session initiation requests

Rule: Value cannot be 0.

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rules: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select true if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUId)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUId)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (personalCertDN)

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for configuring secure proxy administrative agents using the zpmt command

The **zpmt** command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a secure proxy administrative agent

Tip: See the sample response file in the *app_server_root/zOS-config/zpmt/samples* directory.

Server type

Server type (serverType)

Type of server to be created within this management profile

Profile information

Profile name (profileName)

The profile name is default.

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as config_hlq) to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 8.5:

```
SYSPROG1.WAS85.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS85.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS85.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)**Allow OS security to assign GID (zServantGroupGID)**

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)**Allow OS security to assign GID (zLocalUserGroupGID)**

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations**System name (zSystemName)**

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization**Mount point (zConfigMountPoint)**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset name.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

See "Product file system" on page 20 for more information.

Volume, or '*' for SMS (zConfigHfsVolume)

Specify either the DASD volume serial number to contain the above dataset or * to let SMS select a volume. Using * requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle dataset allocation automatically, list the volume explicitly.

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

System information**Product file system directory (zSmpePath)**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read "Product file system" on page 20 for more information.

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasInstall.

Server customization**Short cell name (zCellShortName)**

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must be seven or fewer characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.

Cluster transition name (zClusterTransitionName)

WLM APPL ENV (WLM application environment) name for this server

Rule: Name must be eight or fewer characters and all uppercase.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server address space information customization

In the following, names must be eight or fewer characters unless specified otherwise.

Controller information**Procedure name (zControlProcName)**

Name of member in your procedure library to start the controller

Rule: Name must be seven or fewer characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Servant information**Procedure name (zServantProcName)**

Name of member in your procedure library to start the servant

Rule: Name must be seven or fewer characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

Note: The node host name must always resolve to an IP stack on the system where the application server runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Bootstrap port (zBootstrapPort)

Port for IIOp requests that acts as the bootstrap port for this server (BOOTSTRAP_ADDRESS)

Rule: Value cannot be 0.

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses local comm communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOp IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must be seven or fewer characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Use virtual keyring for z/OS SSL clients (zUseVirtualKeyring)

Select true if you want to enable z/OS SSL clients using SAF Virtual Key Ring to connect to this WebSphere Application Server node without requiring each user to have the WebSphere Application Server keyring or the WebSphere Application Server CA certificate connected to it.

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (`zSecurityDomainId`)

Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

Administrator user ID (`zAdminUserid`)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (`zAdminUid`)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Unauthenticated User ID (`zAdminUnauthenticatedUserid`)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (`zAdminUnauthenticatedUid`)

Valid UID for this user ID

Rule: UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enable writable SAF keyring support (`zEnableWritableKeyring`)

Select `true` if you want to enable writable SAF key ring support

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (`adminUserName`)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (`adminPassword`)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Default personal certificate

Issued to distinguished name (`personalCertDN`)

Identifier of the personal certificate

Issued by distinguished name (`signingCertDN`)

Identifier of the root signing certificate

Expiration period in years (`personalCertValidityPeriod`)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Using installation verification tests

You initially run the installation verification test (IVT), which verifies that WebSphere Application Server is configured correctly for your system, during customization of each of your systems.

Before you begin

If you want to run the IVT at a time other than during initial customization, however, there are two methods from which you can choose.

Note: These options are now available when you are running a standalone application server configuration as well as after federating an application server.

Procedure

Select either method to invoke the IVT:

- “Running installation verification tests with jobs”
- “Running installation verification tests from a command line” on page 534

Running installation verification tests with jobs

The installation verification test (IVT) can be run in three steps.

Before you begin

The application server must be running when you initiate the test.

Procedure

1. Verify that the application server is running.
2. Confirm that the ivtApp application is installed and started.
3. Submit the job BBOWIVT.

Results

The IVT runs a series of verification tests and reports pass or fail status for each in the messages generated by the BBOWIVT job. The output is written to the job output for the submitted BBOWIVT JCL and to the `was_home/profiles/default/logs/ivtClient.log` file.

Running installation verification tests from a command line

You can run the installation verification test (IVT) to get reports on pass or fail status for each in the messages generated by the BBOWIVT job.

Before you begin

The application server must be running when you initiate the test.

Procedure

1. Verify that the application server is running.
2. Confirm that the ivtApp application is installed and started.
3. From a command line, navigate to the *was_home/bin* directory.
4. Issue the following command:

```
ivt.sh server_name profile_name -p port_number [-host host_name]
```

where

- *server_name* is the short name of the server.
- *profile_name* is the name of the profile.
- *-p port_number* is an argument that specifies the port number.
- *-host host_name* is an optional argument that specifies the host name. If you do not specify a host name, the program will use the host-name value that is set in your TCP/IP hosts file.

Example:

```
/WebSphere/V8R5/AppServer/bin> ivt.sh serverj default -p 9080 -host myhost
```

Results

The IVT runs a series of verification tests and reports pass or fail status for each in the messages generated by the BBOWIVT job. The output is written to standard output and to the *was_home/profiles/default/logs/ivtClient.log* file.

switchModules command

Beginning with WebSphere Application Server for z/OS Version 7.0, the load modules are in the product file system. You can use the **switchModules** command to switch a configuration between using load modules in the file system and using load modules in a dataset.

Note: The *server_dlls_in_hfs* environment variable must also be set to 0 for the server to use the DLLs that have been put into a dataset that is in STEPLIB, LPA, or link list.

Location

The *switchModules.sh* shell script is located in the *smpe_install_root/bin* or *app_server_root/bin* directory.

Syntax

```
switchModules.sh target_was_home  
                 target_dataset_name  
                 (dll_optimization)
```

Parameters

target_was_home

Home directory of the node that is the target of the switch

This parameter is required.

target_dataset_name

Dataset name of a PDS-E dataset to which the WebSphere Application Server load modules should be written

This parameter is required.

dll_optimization

Specifies the type of hardware for which DLLs are optimized

This parameter is optional.

OPTBASE

Specifies that DLLs that are optimized for lowest level of hardware that is allowed for this version of Websphere Application Server be returned

This is the default if a value for *dll_optimization* is not specified.

OPT9 Specifies that DLLs that are compiled with ARCH(9) be returned

These optimized DLLs can be used when running on a zEnterprise 196 (machine type 2817) system.

Chapter 10. Updating and uninstalling the product on z/OS

You can use IBM Installation Manager to update or uninstall the WebSphere Application Server for z/OS product.

Optional features

Certain product features can be added or removed from an installed copy of the WebSphere Application Server product. These are called optional features. Choose the optional features for each copy of the WebSphere Application Server for z/OS code according to your needs.

See “Adding and removing features on z/OS.”

Language packs

Parts of the WebSphere Application Server product are provided in translated form in a number of languages. English messages and panels are always installed. You can specify additional languages for which panels and messages are to be added to the product. All products installed at a particular location by IBM Installation Manager share the same list of installed languages, but not all languages are supported by all products.

See “Adding language packs on z/OS” on page 539.

Product maintenance

IBM regularly provides updates to the WebSphere Application Server product to fix product defects and add new function. Product fix packs contain bundled service to bring WebSphere Application Server up to a new product level. Interim fixes provide updates to correct individual product defects. See “Installing interim fixes and fix packs on z/OS operating systems” on page 541.

Uninstalling the product

You can use IBM Installation Manager to uninstall individual copies of WebSphere Application Server product code.

See “Uninstalling the product on z/OS” on page 545.

Adding and removing features on z/OS

Use IBM Installation Manager to add and remove features for the WebSphere Application Server for z/OS product.

Before you begin

Obtain the product repository for WebSphere Application Server for z/OS Version 8.5. 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 for z/OS can have a different set of installed features.

The following features are available for the WebSphere Application Server base product. The keyword name for each feature is provided in parentheses.

- WebSphere Application Server full profile (`core.feature`)

Installing this application-server feature gives you the traditional standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation, offering broad programming model choice and low total cost of ownership through high performance and high manageability.

- EJBDeploy tool for pre-EJB 3.0 modules (`ejbdeploy`)

This optional feature contains the EJBDeploy tool for pre-EJB 3.0 modules.

Before you deploy applications on the server, you must run the EJBDeploy tool on applications that contain EJB modules that are based on specifications prior to EJB 3.0. Running the EJBDeploy tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature called JITDeploy, which automatically generates code when the application starts.

- Standalone thin clients and resource adapters (`thinclient`)

This optional feature contains the IBM standalone thin clients and resource adapters. IBM thin clients provide a set of clients for a variety of technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.

- Embeddable EJB container (`embeddablecontainer`)

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 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.

- Sample applications (`samples`)

This optional feature contains the PlantsByWebSphere sample application. The samples feature is recommended for installation in learning and demonstration environments, such as development environments; however, it is not recommended for installation in production application server environments.

- WebSphere Application Server Liberty profile (`liberty`)

Installing this application-server feature gives you a lightweight profile of the application server along with a simplified configuration approach for the development environment. Its fast restart times, small size, and ease of use make it a good option for building web applications that do not require the full JEE environment of traditional enterprise application server profiles. The Liberty profile also can be used in production; and because it is a dynamic configuration, the application server provisions only the features required by the running applications.

Notes:

- You must install `core.feature` (full WebSphere Application Server profile), `liberty` (Liberty profile), or both.
- You cannot use the Installation Manager modify, update, or rollback functions to modify this installation later and add or remove `core.feature` (full WebSphere Application Server profile) or `liberty` (Liberty profile). You can use these functions to add or remove the `ejbdeploy`, `thinclient`, `embeddablecontainer`, or `samples` subfeature of `core.feature` 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 for z/OS and do not specify the features to be installed, the following features are installed by default:

- core.feature
- ejbdeploy
- thinclient
- embeddablecontainer

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 `imc1` install command. For example, the following command:

```
imc1 install com.ibm.websphere.zOS.v85,core.feature,samples,thinclient
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
```

would install the product with the `core.feature`, `samples`, and `thinclient` features but not the `ejbdeploy`, `embeddablecontainer`, or `liberty` features.

4. To add one or more features to an existing product installation, issue the `imc1` install command and specify the features to be added, separated by commas, after the offering name.

For example:

```
imc1 install com.ibm.websphere.zOS.v85,embeddablecontainer
-installationDirectory installation_location
-repositories list_of_repository_locations
```

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 `imc1` uninstall command and specify the features to be removed, separated by commas, after the offering name.

For example:

```
imc1 uninstall com.ibm.websphere.zOS.v85,samples,thinclient
-installationDirectory installation_location
```

This will uninstall the `samples` and `thinclient` optional features.

Note: Before uninstalling 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 WebSphere Application Server nodes and servers.

What to do next

Customize or make use of any new features that you added.

Adding language packs on z/OS

Use IBM Installation Manager to add non-English language packs when you install the WebSphere Application Server for z/OS product. On z/OS, language packs provide translated administrative console panels and messages for additional languages.

Before you begin

Obtain the product repository for WebSphere Application Server for z/OS Version 8.5. The following instructions assume that the repository is mounted at `/usr/lpp/InstallationManagerRepository/HBB0850`. The repository can be mounted read-only.

Decide which language packs you need.

- Brazilian Portuguese (`pt_BR`)

- Chinese, Simplified (zh_TW)
- Chinese, Traditional (zh)
- Czech (cs)
- English (en)
- French (fr)
- German (de)
- Hungarian (hu)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Polish (pl)
- Romanian (ro)
- Russian (ru)
- Spanish (es)

Each installed copy of WebSphere Application Server for z/OS can have a different set of installed language packs.

There are no language packs for DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS or Web Server Plug-ins for IBM WebSphere Application Server for z/OS.

Procedure

1. Mount the product file system for the product which is being installed.
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. When you install the product, specify the `cic.selector.nl` property on the `imcl` install command.

The property should be set to the list of locales corresponding to the desired language packs. Separate the locale entries with double commas, and do not enclose the list in quotes.

For example, the following command:

```
imcl install com.ibm.websphere.zOS.v85
-installationDirectory /usr/lpp/zWebSphere/V8R5
-properties cic.selector.nl=de,,zh
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-acceptLicense
```

would install the product with the language packs for English, German, and Traditional Chinese.

Note: It is not necessary to specify English. English is always installed.

This also sets the list of languages for any other products that are installed at the same location or will be installed there in the future.

Note: If you specify new language packs when installing an additional product at an existing location, all products already installed at that location will be updated to include their own language packs for the new languages. As a result, you should make the repositories for other products available to Installation Manager when adding language packs to a package group containing other products.

4. Unmount the product file system and remount it read-only for use by WebSphere Application Server nodes and servers.

What to do next

You can now use the administrative console in the selected languages.

Installing interim fixes and fix packs on z/OS operating systems

Product fix packs contain bundled service to bring WebSphere Application Server up to a new product level. Interim fixes provide corrective service for specific known problems. You can use IBM Installation Manager to update the product with the fixes that are available for your service level of WebSphere Application Server Version 8.5.

Before you begin

Contact the IBM Software Support Center for information about upgrades for WebSphere Application Server 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.

IBM Installation Manager is used to apply product maintenance to WebSphere Application Server for z/OS. A set of scripts called the **post-installer**, a part of WebSphere Application Server for z/OS, is used to make any configuration file system changes that are required as a consequence of product maintenance.

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 or later.

Procedure

1. Use Installation Manager to apply the required maintenance to your product dataset and file-system structure.
 - a. For a list of fixes that are available for WebSphere Application Server Version 8.x 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** as the product.
 - 4) Select the version of the product to be updated (8.x.x.x).
 - 5) Select your operating system 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 Version 8.x with the fixes using one of the following procedures.
 - To update the product 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 Version 8.x 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 Version 8.5 product offerings for supported operating systems” on page 5.

- 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:

- 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 an Installation Manager credentials file containing your IBM software user ID and password, create one that will allow you to access the repository.

Note: These are the credentials that you use to access protected IBM software websites.

Use the `imutilsc saveCredential` command to create a keyring or add additional credentials to it:

```
imutilsc saveCredential
-keyring keyring_file
-username IBM_software_ID
-userPassword IBM_software_password
-url repository_URL
```

For information on the `imutilsc saveCredential` command, read the IBM Installation Manager Version 1.5 Information Center.

Tip: When creating a keyring 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.

- 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 product_installation_location
-repositories repository_URL
-keyring keyring_file
```

To install a fix pack, use this command:

```
imcl install offering_ID_offering_version
-installationDirectory product_installation_location
-repositories repository_URL
-keyring keyring_file
-acceptLicense
```

Tips:

- The `offering_ID` is the offering ID that is listed in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 5.
- 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.

c) **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

- To update the product 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 Version 8.x 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** as the product.
 - d) Select the version of the product to be updated (8.x.x.x).
 - e) Select your operating system 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 product_installation_location
      -repositories compressed_file
```

To install a fix pack, use this command:

```
imcl install offering_ID_offering_version
      -installationDirectory product_installation_location
      -repositories location_of_expanded_files
      -acceptLicense
```

Tips:

- The `offering_ID` is the offering ID that is listed in “WebSphere Application Server Version 8.5 product offerings for supported operating systems” on page 5.

- 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.

iii. **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

- To update the product 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 product to the SMP/E-managed repository that contains the base product by applying PTFs for the fix pack to the repository. See the WebSphere Application Server 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 Version 8.x with the new fix pack.

- 1) Apply the PTFs for the fix pack to the WebSphere Application Server Version 8.5 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 product fix-pack level. For example:

```
imcl install com.ibm.websphere.zOS.v85_offering_version
-installationDirectory product_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 product is installed for use with WebSphere Application Server Version 8.5, it is installed into the WebSphere Application Server product file system.

iii. **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

For more information on updating WebSphere Application Server, see Chapter 10, “Updating and uninstalling the product on z/OS,” on page 537.

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 start-up, 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 product on z/OS

Use IBM Installation Manager to uninstall copies of the product code for WebSphere Application Server for z/OS, DMZ Secure Proxy Server for IBM WebSphere Application Server for z/OS, Web Server Plug-ins for IBM WebSphere Application Server for z/OS, or IBM HTTP Server for WebSphere Application 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.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.

Chapter 11. Centralized installation manager (CIM)

Use the centralized installation manager (CIM) to shorten the number of steps that are required to create and manage environments that contain WebSphere Application Server Version 6.1.x, 7.x, and 8.x.

Before you begin

The process for managing Version 7.x and previous versions is different from the process for managing Version 8.x. The following topic explains the different CIM usage scenarios.

About this task

The Version 8.5 Centralized Installation Manager (CIM) can be used to manage Version 8.5 and previous versions of WebSphere Application Server. You can use CIM to install or uninstall Version 8.5 and previous versions of WebSphere Application Server on remote machines and apply maintenance from the administrative console. In Version 8.0 and later, targets can be added outside of the cell. The process for managing Version 7.x and previous versions is different from the process for managing Version 8.x, and each process is documented separately in the information center.

Note: The process for managing the centralized installation manager (CIM) for WebSphere Application Server Version 6.1.x and 7.x is different from the process for managing Version 8.x, and each process is documented separately in the information center. For Version 8.x, CIM uses the Installation Manager to install the product on remote machines. For Version 6.1.x and 7.x, CIM uses the ISMP and Update Installer.

- To get started using CIM for Version 8.5, see “Submitting Installation Manager jobs” on page 548

Table 546. Differences between CIM for Version 8.x and CIM for Version 6.1.x and 7.x

Function	CIM Version 6.1.x and 7.x	CIM Version 8.x
Scope	Install, update, uninstall Version 7.x. Update Version 6.1.x* *(Not supported on z/OS targets.)	Install, update, uninstall Version 8.x and all Installation Manager installable products: WebSphere Application Server, IHS Plugin, and DMZ. Targets can now be added outside of the cell.
Installation software used	ISMP and Update Installer	Installation Manager
Repository	Maintains a private repository on the Deployment Manager	Maintains an installation kit directory. Uses Installation Manager repository
Administrative console	Accessible from the Deployment Manager	Accessible from the Job Manager. Job Manager is also available on the Deployment Manager
Command line	CIM AdminTask commands	Use the Job Manager's submitJob command

Procedure

1. For Version 8.x, CIM functions are accessed through the job manager or deployment manager. Using the job manager or deployment manager, you can perform the following functions:

- Install, update, and uninstall IBM® Installation Manager on remote machines*
- Install, update, and uninstall WebSphere Application Server Version 8.x offerings on remote machines
- Collect, distribute, and delete files on remote hosts
- Run scripts on remote hosts
- Manage profiles on remote hosts for WebSphere Application Server*

*(Not supported on z/OS targets.)

Version 8.0 and later, CIM offers the following improvements over previous versions:

- Support for z/OS operating system targets
- Removal of cell boundary limitations. Targets can now be added outside of the cell.

- Job scheduling
2. For Version 6.1.x and 7.0, CIM functions are accessed using the deployment manager. CIM functions with Version 6.1.x and 7.0 are not supported for z/OS operating system targets. Using the deployment manager, you can perform the following functions:
 - Install, update, and uninstall WebSphere Application Server Network Deployment Version 7.x on remote machines
 - Install and uninstall WebSphere Application Server Version 6.1.x and 7.x refresh packs, fix packs, and interim fixes on remote machines

Submitting Installation Manager jobs

In a flexible management environment, you can submit jobs to install Installation Manager instances, update Installation Manager with a repository (not supported on z/OS targets), manage Installation Manager offerings, and install WebSphere Application Server Version 8.5 products.

Before you begin

Note: This topic applies to WebSphere Application Server Version 8.5.

Start the job manager and make a remote host a target of the job manager. In the job manager console or deployment manager console, click **Jobs > Targets > New Host** and complete the fields on the New targets page.

A remote host typically is a different computer than the one on which the job manager is installed.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must be applicable to all of the job targets.

SSH code is not automatically included with z/OS operating systems. You must ensure SSH is installed and enabled on any target you want to access using CIM.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

For Version 8.0 and later, centralized installation manager (CIM) functions are accessed through the job manager. Using the job manager, you can perform the following functions:

- Install, update, and uninstall WebSphere Application Server offerings on remote machines
- Install, update, and uninstall IBM Installation Manager on remote machines. Not supported on z/OS targets. For z/OS targets, you must install Installation Manager prior to working with CIM.
- Collect, distribute, and delete files on remote hosts
- Run scripts on remote hosts

For Version 8.x, CIM functions are not compatible with CIM Version 6.x or 7.x.

Note: IBM Installation Manager 1.5.2 or above is required.

About this task

You can use the Installation Manager to install and manage installations on remote hosts. Using the job manager, you can run jobs that create and update Installation Manager instances and install the product on remote hosts.

The topics in this section describe how to use the Installation Manager by running jobs in the job manager console or the deployment manager console. Instead of using a console, you can run wsadmin commands in the AdministrativeJobs command group. See the Administrative job types topic.

Procedure

- Run the install Installation Manager job.
- Run the update Installation Manager job.
- Run the uninstall Installation Manager job.
- Run the install SSH public key job.

Note: If your remote target is running a Tectia SSH server and it does not support the use of SCP file transfer protocol, some CIM jobs may fail during file transfer. To avoid this problem, you can force the file transfer to use SFTP instead of SCP. In order to use the SFTP mode, set the java system property "com.ibm.ws.admin.cim.rxa.force.sftp" to "true." If this property is not set, or set to "false", then the file transfer default is SCP. For CIM Version 7.0 and 8.0, you can use the following wsadmin command to set the java property:

```
AdminTask.setJVMSystemProperties('[-propertyName com.ibm.ws.admin.cim.rxa.force.sftp  
-propertyValue true]') AdminConfig.save()
```

You must then restart the server.

Using CIM Version 8.0, you can also specify to use SFTP for each target individually. When registering the target host, set the host property "com.ibm.ws.admin.cim.rxa.force.sftp" to "true." Use the following wsadmin command:

```
AdminTask.registerHost('[-host thinkblue -hostProps [ [com.ibm.ws.admin.cim.rxa.force.sftp true]  
[osType os_type] [password password] [saveSecurity true] [username user_name] ]]')
```

The host property value takes precedence.

What to do next

On the Job status page, click the ID of the job and view the job status. If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

To review the Installation Manager license, perform the following steps:

- If you are using the graphical user interface (GUI), run the following command and follow the instructions:
- If you are using the command line, run the following command and follow the instructions:

Submitting jobs to install Installation Manager on remote hosts

In a flexible management environment, you can submit the **Install IBM Installation Manager** job to install the Installation Manager on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to install Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply to all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

For instructions on updating an existing instance of Installation Manager, see Submitting jobs to update Installation Manager on remote hosts.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Install IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the installIM job script in the AdministrativeJobs command group. See the Administrative job types topic.

For Windows targets, CIM sends unzip.exe to the target to unzip the Installation Manager zip file. If you do not want to use unzip.exe from CIM, you can set the JVM parameter:

```
com.ibm.ws.admin.cimjm.unzipOnTheFly=true/TRUE"
```

If this parameter is set to true, CIM unzips the zip file from the job manager and sends individual files to the target. You must restart the server after changing this parameter.

For Linux/UNIX targets, if CIM detects an instance of unzip, CIM sends the zip file to the target and then unzips the zip file. If CIM does not detect an instance of unzip, CIM unzips the zip file from the job manager and sends individual files to the target. Sending the files individually usually requires more time than unzipping on the target. For IBM i targets, CIM uses the jar command found on the IBM i target to unzip the zip file.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.5.2 or above is required.

Procedure

1. Click **Jobs > Submit** from the navigation tree of the administrative console.
2. Choose the **Install IBM Installation Manager** job and click **Next**.
3. Choose job targets.
 - a. Select a group of targets from the list, or select **Target names**.
 - b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
 - c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
 - d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to install.

Note: If you do not specify the IBM Installation Manager installation kit path, the installIM job searches for the most recent IBM Installation Manager installation kit that is suitable for the target platform from the installation kit repository on the Job Manager. By default, the installation kit

repository is <profile_home>/IMkits. You can change the location from the Job Manager. Click **Jobs > Installation Manager installation kits**, then modify 'Installation Manager installation kits location' to a different location. If you are using the command line, you can check for the repository location at: <profile_home>/properties/cimjm/CIMJMetadata.xml.

Optional parameters:

- Installation Manager agent data location: specifies the location of the Installation Manager agent data.

Note: The data location cannot be a subdirectory of the installation location.

- Installation Manager installation directory: specifies the location of the Installation Manager installation directory.

If you select the **Skip prerequisite checking** check box, you specify that no prerequisite checking is performed when installing Installation Manager and that Installation Manager disk space checking is disabled. For the job to run successfully, you must select **I accept the terms in the license agreements**. Click **Next**

To review the Installation Manager license, perform the following steps:

Note: Run the install command from the Installation Manager install kit.

- If you are using the graphical user interface (GUI), run the following command and follow the instructions:
- If you are using the command line, run the following command and follow the instructions:

To install Installation Manager so that it can be used by a group of users, specify the **installType** optional parameter. Values for the parameter include:


- single: perform a single user installation in non administrative mode. This option is available for all CIM supported platforms.
- Auto: the command initiates a single user installation in non administrative mode if you are a non administrative user. If you are an administrator, this action performs an administrative installation.

5. Schedule the job, and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and installs Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon  to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to update Installation Manager on remote hosts for Version 8.5

In a flexible management environment, you can submit the **Update IBM Installation Manager** job to update the Installation Manager on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to update Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

To review the Installation Manager license, perform the following steps:

- If you are using the graphical user interface (GUI), run the following command and follow the instructions:
- If you are using the command line, run the following command and follow the instructions:

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Update IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the updateIM job script in the AdministrativeJobs command group. See the Administrative job types topic.

Note: IBM Installation Manager 1.5.2 or above is required.


Procedure

1. Click **Jobs > Submit** from the navigation tree of the administrative console.
2. Choose the **Update IBM Installation Manager** job and click **Next**.
3. Choose job targets.
 - a. Select a group of targets from the list, or select **Target names**.
 - b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
 - c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
 - d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to update and the location of the repository that contains the update. For the job to run successfully, you must select **I accept the terms in the license agreements**. Click **Next**. You can also update Installation Manager using an installation kit. Specify the existing installation location. Select the **Update existing installation** check box. If updating with an Installation Manager installation kit, specify the fully qualified local path and file name of the installation kit. If the field is left blank, the update IBM Installation Manager job will locate and use the most recent IBM Installation Manager installation kit available in the default location for installation kits: \$JOB_MANAGER_HOME/IMKit.
5. Schedule the job and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and updates Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon  to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to uninstall Installation Manager on remote hosts

In a flexible management environment, you can submit the **Uninstall IBM Installation Manager** job to remove the installation manager from registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to remove Installation Manager are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role . When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the console, choose the **Uninstall IBM Installation Manager** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the manageOfferings job script in the AdministrativeJobs command group. See the Administrative job types topic.


Procedure

1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Uninstall IBM Installation Manager** job and click **Next**.
3. Choose job targets.
 - a. Select a group of targets from the list, or select **Target names**.
 - b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
 - c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
 - d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the Installation Manager instance that you want to uninstall. Click **Next**.
5. Schedule the job and click **Next**.
6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and uninstalls Installation Manager on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon  to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Submitting jobs to install SSH public keys on remote hosts

In a flexible management environment, you can submit the **Install SSH Public Key** job to install SSH public keys on registered hosts of the job manager.

Before you begin

Start the job manager and the targets. Ensure that the targets for which you want to install an SSH public key are registered with the job manager.

To submit jobs, your ID at the job manager must be authorized for the administrator role or the operator role. When you submit a job, you can specify a user name and password for authentication and authorization at the target or targets. When you submit a job to multiple targets, the user name and password or the credentials for the submitter must apply all of the job targets.

To run the job against a large number of targets, optionally create a group of targets and submit the job against the group.

Note: IBM Installation Manager 1.4.3 or above is required.

About this task

You can use the administrative console of the job manager or the deployment manager to submit the job. From the job manager console, choose the **Install SSH Public Key** job, specify the targets, schedule the job, review the summary, and submit the job.

Instead of using a console, you can run the Install SSH Public Key job script in the AdministrativeJobs command group. See the Administrative job types topic.

Procedure


1. Click **Jobs** > **Submit** from the navigation tree of the administrative console.
2. Choose the **Install SSH Public Key** job and click **Next**.
3. Choose job targets.
 - a. Select a group of targets from the list, or select **Target names**.
 - b. If you selected **Target names**, then specify a target name and click **Add**, or click **Find** and specify the chosen targets on the Find targets page.
 - c. If user authentication is required, specify a user name, password, or any other authentication values as needed.
 - d. Click **Next**.
4. On the Specify the job parameters page, specify the location of the public key file that you want to install on the selected target. Click **Next**.
5. Schedule the job and click **Next**.

6. Review the summary, and click **Finish** to submit the job.

Results

The job runs and installs a public key file on the selected targets.

What to do next

On the Job status page, click the job ID and view the job status. Click the status refresh icon  to refresh the displayed job status.

If the job is not successful, view any error messages that result from running the job, correct the error condition, and submit the job again.

Installing the Version 8.5 product using the job manager and administrative console

In a flexible management environment, you can use the job manager to install, update, and uninstall IBM WebSphere Application Server using the graphical user interface.

Before you begin

Note: This topic applies to WebSphere Application Server Version 8.5. For information about using centralized installation manager (CIM) for Version 6.1.x and 7.x, see the topic about getting started with the centralized installation manager (CIM) for previous versions..

Ensure that you have the administrative console installed on your primary machine.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

About this task

To install WebSphere Application Server, use the administrative console to register your target machine, install IBM Installation manager, and install WebSphere Application Server or other product offerings that are compatible with Installation Manager. Using the administrative console, you can set parameters for the directory in which to install the product on the target machine, specify where to store product data on the target machine, and specify the URL of the repository to download the product from. Depending on your security setup, you can also specify keyring credentials to log in to the product repository.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.5.2 or later is required.

Procedure

1. Start the job manager. See Starting the job manager.
2. Register a host with the job manager. Before you can install the product on a target machine, you must register it with the job manager. For more information, see Register or unregister with job manager settings.
3. Launch the administrative console. For more information, read about the administrative console.
4. Test the connection to the targets on which you want to install the product. This step is optional. Before you install the product on a target machine, you can test the connection.

- a. In the administrative console, select **Job > Submit**.
 - b. In the Job type menu list, select **Test connection**. Click **Next**.
 - c. Specify the target names and target authentication.
 - If you test the connection without specifying credentials, the test will use default to existing credentials.
 - You can submit the **Test connection** job with a user name and password.
 - You can submit the **Test connection** job with a user name and private key file.
5. Optionally run an inventory job. To see what is installed on your target machine, you can run an inventory job.
- a. In the administrative console, select **Job > Submit**.
 - b. In the job type menu list, select **Inventory**. Click **Next**.
 - c. Specify the target names and target authentication.
 - You can submit an inventory job with a user name and password.
 - You can submit an inventory job without a user name and password.
6. Install or update Installation Manager on your target machine. This step is optional. If you already have the correct version of Installation Manager on your target machine, you can proceed to the next step. For more information, see Managing Installation Manager using the job manager. This step does not apply to zOS targets.
7. If you use secure shell (SSH) security, install your public key file. You can install the public key file using the same credentials as the job manager. This step does not apply to IBM i targets.
- a. In the administrative console, select **Job > Submit**.
 - b. In the job type drop down menu, select **Install SSH Public Key**. Click **Next**.
 - c. Specify the job parameters.
8. Install the product. Use the manageOfferings job to install the product.
- a. In the administrative console, select **Job > Submit**.
 - b. In the job type drop down menu, select **Manage offerings**. Click **Next**.
 - c. Specify the following optional or required job parameters.

Required parameter:

 - Response file path name: The full path name to the response file on the job manager machine.

Optional parameters:

 - IBM Installation Manager Path: Specify the path to install Installation Manager on the remote machine. If this parameter is blank, then Installation Manager is installed to the default location.
 - IBM Installation Manager key ring file: If the package repository requires a key ring file for authentication, specify the full path name of the key ring file on the job manager machine.
 - Key ring file password: If the key ring file is password protected, specify the key ring password.
 - IBM Installation Manager agent data location: Specify an IBM Installation Manager data location that is not the default location for the manageOfferings job.

Note: Do not use a non-default data location unless you are familiar with IBM Installation Manager.
 - d. Select **I accept the terms in the license agreements**.
9. Optionally transfer files to or from the target machine. For example, if the installation fails, you might want to transfer the log files from the target machine to understand why the job failed.
- To collect a file from remote hosts:
 - a. In the administrative console, select **Job > Submit**.
 - b. In the job type menu list, select **Collect file**. Click **Next**.
 - c. Specify the job parameters.

- The destination location is <profile home>/config/temp/JobManager/<task id>/<host name>.
 - To distribute a file to remote hosts:
 - a. In the administrative console, select **Job > Submit**.
 - b. In the job type menu list, select **Distribute file**. Click **Next**.
 - c. Specify the job parameters.
 - The source location must be <profile home>/config/temp/JobManager.
 - To delete a file on remote hosts:
 - a. In the administrative console, select **Job > Submit**.
 - b. In the job type menu list, select **Remove file**. Click **Next**.
 - c. Specify the job parameters.
10. Create a profile for the newly installed product on the target machine.
 - a. In the administrative console, select **Job > Submit**.
 - b. In the job type menu list, optionally select **Manage Profiles**. Click **Next**.
 - c. Choose the job targets.
 - d. Specify the job parameters.
 - wasHome: The directory where you installed the product on the target machine
 - responseFile: The response file used to create an IBM WebSphere Application Server profile

Results

You have installed WebSphere Application Server on a target machine and created a profile using the job manager.

What to do next

Using the job manager, you can run any command or script on your target machine.

1. In the administrative console, select **Job > Submit**.
2. In the job type drop down menu, select **runCommand**. Click **Next**.
3. Specify the job parameters.

You can uninstall Installation Manager using the administrative console. For more information, see [Managing Installation Manager using the job manager](#).

Installing the Version 8.5 product using the job manager and command line

In a flexible management environment, you can use the job manager to install, update, and uninstall IBM WebSphere Application Server using the command line with a response file.

Before you begin

Before you install WebSphere Application Server using the job manager, ensure that you have WebSphere Application Server Version 8.5 installed on your primary machine.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

About this task

To install WebSphere Application Server, use `wsadmin` to run the `manageOfferings` command. The `manageOfferings` command uses a response file and a security keyring. In the response file, you can set parameters for the directory in which to install the product on the target machine, specify where to store product data on the target machine, and specify the URL of the repository to download the product from. Depending on your security setup, you can also specify keyring credentials to log in to the product repository.

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

Note: IBM Installation Manager 1.5.2 or later is required.

Procedure

1. Start the job manager. For detailed instructions, see starting the job manager.
2. Register a host with the job manager. Before you can install the product on a target machine, you must register it with the job manager. Use the `wsadmin` tool to run the `registerHost` command.
 - You can register the host with a private key; for example:
 - Using Jacl:

```
$AdminTask registerHost {-host hostname -hostProps
  {{privateKeyFile filename} {username root }{saveSecurity true}}}
```
 - Using Jython:

```
AdminTask.registerHost('[-host hostname -hostProps
  [[username user][privateKeyFile filename][saveSecurity true]]]')
```
 - You can register the host with a user name and password; for example:
 - Using Jacl:

```
$AdminTask registerHost {-host hostname -hostProps { {password xxxxx}
  { username root } {saveSecurity true}}}
```
 - Using Jython:

```
AdminTask.registerHost('[-host hostname -hostProps [[password xxxxx][username user]
  [saveSecurity true]]]')
```
3. Optional: Test the connection to the targets on which you want to install the product. Before you install the product on a target machine, you can test the connection.
 - If you test the connection without specifying credentials, the test will use default to existing credentials; for example:
 - Using Jacl:

```
$AdminTask submitJob {-jobType testConnection -targetList {hostname}}
```
 - Using Jython:

```
AdminTask.submitJob('-jobType testConnection -targetList [hostname]')
```
 - You can submit the Test connection job with a username and password; for example:
 - Using Jacl:

```
$AdminTask submitJob {-jobType testConnection -targetList
  {hostname} -username username -password password}
```
 - Using Jython:

```
AdminTask.submitJob('-jobType testConnection -targetList
  [hostname] -username username -password password')
```
 - You can submit the Test connection job with a user name and private key file; for example:
 - Using Jacl:


```
$AdminTask submitJob {-jobType testConnection -targetList
{hostname} -username username -privateKeyFile private_key_filename}
```

– Using Jython:

```
AdminTask.submitJob('-jobType testConnection -targetList
[hostname] -username username -privateKeyFile C:\temp\private_key_filename')
```

4. Optionally run an Inventory job to see what is installed on your target machine.

a. Submit an Inventory job with a user name and password.

• Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname}
-username username -password password}
```

• Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname]
-username username -password password')
```

b. Submit an Inventory job without a user name and password.

• Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname}}
```

• Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname]')
```

5. Optional: Install or update Installation Manager on your target machine.

If you already have the correct version of Installation Manager on your target machine, you can proceed to the next step. For more information, see managing Installation Manager using the job manager.

6. If you use SSH security, install your public key file.

You can install the public key file using the same credentials as the job manager. This step does not apply to IBM i targets.

a. Run the installSSHPublicKey admin task; for example:

• Using Jacl:

```
$AdminTask submitJob {-jobType installSSHPublicKey -targetList {target}
-jobParams { {publicKeyFile keyfilepath} } -description "test installSSHPublicKey"}
```

• Using Jython:

```
AdminTask.submitJob ('-jobType installSSHPublicKey -targetList [target]
-jobParams [[publicKeyFile keyfilepath]] -description "test installSSHPublicKey"')
```

7. Set up a response file for the **manageOfferings** command.

a. Create a response file. You can create a response file using the Installation Manager. For more information, see creating a response file with Installation Manager.

b. You can edit the response file to include information about your target machine.

c. You can use the response file to install any offering that is compatible with Installation Manager. For more information, see the Installation Manager information center.

a. Save the response file as filename.txt.

8. Run the **manageOfferings** command. For the job to run successfully, you must specify `acceptLicense TRUE`.

a. Open `wsadmin` from the job manager profile bin directory.

b. Enter the **manageOfferings** command in `wsadmin`. For example:

• Using Jacl:

```
$AdminTask submitJob {-jobType manageOfferings -targetList hostname -username user -password *****
-jobParams
{{responseFile <RESPONSE FILE LOCATION>} {acceptLicense TRUE} {IMPath <IM install location>}
{keyringFile <key ring file location>} {keyringPassword pwd} }}
```

• Using Jython:

```
AdminTask.submitJob ('-jobType manageOfferings -targetList hostname -username user -password *****
-jobParams
[[responseFile <RESPONSE FILE LOCATION>] [acceptLicense TRUE][IMPath <IM install location>]
[keyringFile <key ring file location>] [keyringPassword pwd]')
```

The `manageOfferings` command pulls the response file that you created in this task and begins the product installation.

The following parameter for this job is required:

- `responseFile`: (Response file path name) This parameter contains the full path name to the offering response file on the job manager machine.

The following parameters for this job are optional:

- a. `IMPath`: (IBM Installation Manager Path) This parameter contains the full path of the IBM installation manager on the remote machine. Use this parameter if you have more than one instance of Installation Manager on your remote machine. If you have only one instance of Installation Manager installed, you can leave this parameter empty because the job can find it. Specify whether the target machine has more than one instance of Installation Manager installed.
 - b. `keyringFile`: (IBM Installation Manager key ring file): If the package repository requires a key ring file for authentication, specify the full path name of the key ring file on the job manager machine.
 - c. `keyringPassword`: (Key ring file password) If the key ring file is password protected, specify the key ring password.
9. Optional: Run the `collectFile` and `distributeFile` administrative tasks.

Optionally transfer files to or from the target machine and delete files on the target machine. For example, if the installation fails, you might want to transfer the log files from the target machine to understand why the job failed. When using these administrative tasks, you can specify wildcards in the filename.

Note: The destination must be a directory, it cannot be a file.

- To collect a file from remote hosts:

– Using Jacl:

```
$AdminTask submitJob {-jobType collectFile -targetList hostname -jobParams
{{source D:\\WAS85\\logs\\manageprofiles\\response.log} {destination log}}}
```

– Using Jython:

```
AdminTask.submitJob('-jobType collectFile -targetList hostname -jobParams
[[source D:\\WAS85\\logs\\manageprofiles\\response.log] [destination log]')
```

- To distribute a file to remote hosts:

– Using Jacl:

```
$AdminTask submitJob{-jobType distributeFile -targetList hostname
-jobParams {{source test.txt}{destination D:\\temp\\test.txt} }}
```

– Using Jython:

```
AdminTask.submitJob('-jobType distributeFile -targetList hostname
-jobParams [[source test.txt][destination D:\\temp\\test.txt] ]')
```

- To delete a file on remote hosts:

– Using Jacl:

```
$AdminTask submitJob{-jobType removeFile -targetList hostname
-jobParams {{location D:\\temp\\test.txt}}}
```

– Using Jython:

```
AdminTask.submitJob('-jobType removeFile -targetList hostname
-jobParams [[location D:\\temp\\test.txt] ]')
```

10. Create a profile for the newly installed product on the target machine.

Restriction: This step does not apply to z/OS targets.

Specify the following parameters:

- `targetList`: The machine where you want to create a new profile
- `wasHome`: The directory where you installed the product on the machine that is running job manager

- responsefile: Enter the directory where you saved your response file. This text file provides the parameters and information of the profile to create.

For example:

- Using Jacl:

```
$AdminTask submitJob {-jobType manageprofiles -targetList hostname
-jobParams {{wasHome D:\\WAS70GA} {responseFile D:\\temp\\mpl.txt}}}
```

- Using Jython:

```
$AdminTask submitJob {-jobType manageprofiles -targetList hostname
-jobParams {{wasHome D:\\WAS70GA} {responseFile D:\\temp\\mpl.txt}}}
```

Results

You have installed the product on a target machine and created a profile using the job manager.

What to do next

Using the job manager, you can run any command or script on your target computer.

- Using Jacl:

```
$AdminTask runCommand {-host hostname -jobParams
{{command command_to_run}{workingDir working_directory_on_remote_host}}}
```

- Using Jython:

```
$AdminTask.runCommand ('-host hostname -jobParams
[[command command_to_run][workingDir working_directory_on_remote_host]]')
```

Managing Installation Manager using the job manager

You can store and manage all of your installation manager installation kits from a central location.

Before you begin

Before you can work with IBM Installation Manager, you must register at least one host with the job manager. You must also have acquired one or more Installation Manager installation kits.

Note: CIM jobs to install, uninstall, and update Installation Manager are not supported on z/OS targets. You must first install Installation Manager on z/OS targets before using CIM manage offerings jobs.

Note: IBM Installation Manager 1.4.3 or above is required.

About this task

If you have multiple Installation Manager offerings or need to manage Installation Manager on multiple remote machines, the job manager can automate this process. Job manager can also store your Installation Manager installation kits in a single repository. This allows you to manage your installation kits from a single location and send your installation kits to multiple machines.

Procedure

- You can submit an inventory job to see what is installed on a host.
 - You can submit an inventory job with a username and password; for example:

- Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname} -username username -password password}
```

- Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname] -username user -password xxxxxx')
```

- If you saved user credentials while registering host, you can submit an inventory job without credentials; for example:

- Using Jacl:

```
$AdminTask submitJob {-jobType inventory -targetList {hostname} }
```

- Using Jython:

```
AdminTask.submitJob('-jobType inventory -targetList [hostname] ')
```

- You can browse the Installation Manager installation kit directory and change the directory location. Perform this task using the administrative console graphical user interface. Open the administrative console and select **Submit Jobs > Installation Manager installation kits**. For more information, see Installation Manager installation kits.
- You can submit a job to install Installation Manager on a host using the administrative console.
 1. In the administrative console, select **Job > Submit**.
 2. In the job type menu list, select **Install IBM Installation Manager**. Click **Next**.
 3. Specify the job parameters. The **Install Action** menu has the following options:
 - Install based on login credentials
 - Install for single user only
 - Install for a group of users
- You can submit a job to install Installation Manager on a host by sending the installation kit from the command line.

The installIM job has the following required parameters:

- **kitPath**: Specify the full path name to the IBM Installation Manager kit on the job manager machine.
- **acceptLicense**: Must be set to true, if you do not specify this parameter, the job will fail.

The installIM job has the following optional parameters:

- **installPath**: Specify the path to install Installation Manager on the remote machine. If this parameter is not specified, then Installation Manager is installed to the default location.
- **dataPath**: Specify the Installation Manager data path on the remote machine. If this parameter is not specified, the default Installation Manager data path is used.
- Submit the install Installation Manager job without credentials; for example:

- Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams { {installPath <path> } {dataPath <path> } {kitPath <path> } {acceptLicense true} } -description "IM install without username"}
```

- Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [[installPath <path>] [dataPath <path>] [kitPath <path>] [acceptLicense true]] -description "IM install without username"')
```

- Submit the install Installation Manager job using a private key; for example:

- Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams { {installPath <path> } {dataPath <path> } {kitPath <path> } {acceptLicense true} } -privateKeyFile "<key file path>" -description "IM install with private key"}
```

- Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [ [installPath <path>] [dataPath <path>] [kitPath <path>] [acceptLicense true] ] -privateKeyFile '<key file path>' -description "IM install with private key"')
```

- Submit the install Installation Manager job using a user name and password; for example:

- Using Jacl:

```
$AdminTask submitJob {-jobType installIM -targetList {hostname} -jobParams { {installPath <path> } {dataPath <path> } {kitPath <path> } {acceptLicense true} } -username root -password abcd -description "IM install with username and pwd"}
```

- Using Jython:

```
AdminTask.submitJob ('-jobType installIM -targetList [hostname] -jobParams [[installPath <path>] [dataPath <path>] [kitPath <path>] [acceptLicense true] ] -username root -password abcd -description "IM install with username and pwd"')
```

- You can review the Installation Manager license.
 - If you are using the graphical user interface (GUI), run the following command and follow the instructions:

- If you are using the command line, run the following command and follow the instructions:
- You can submit a job to update Installation Manager on a host by providing an Installation Manager repository URL from the command line. This job has the following required parameter:
 - acceptLicense: Must be set to true, if you do not specify this parameter, the job will fail.

For example:

- Using Jacl:

```
$AdminTask submitJob {-jobType updateIM -targetList {hostname} -jobParams { {installPath <path>}
{repository <repository URL>} {keyringFile <file path>} {keyringPassword <keyringpwd>} {acceptLicense true} }
-username root -password <password> -description "update IM with username and pwd"}
```

- Using Jython:

```
AdminTask.submitJob('-jobType updateIM -targetList [hostname] -jobParams [ [installPath <path>]
[repository <repository URL>] [keyringFile <file path>] [keyringPassword] [acceptLicense true] ]
-username <username> -password <password>')
```

- You can submit a job to update Installation Manager on a host using the administrative console.
 1. In the administrative console, select **Job > Submit**.
 2. In the job type menu list, select **Update IBM Installation Manager**. Click **Next**.
 3. Specify target names and target authentication.
 4. Specify the job parameters and accept the license agreement:
 - installPath: IBM Installation Manager installation location.
 - repository: IBM Installation Manager repository.
 - keyringFile: IBM Installation Manager key ring file, the credentials for the protected repository are retrieved from the key ring file.
 - keyringPassword: Password for accessing key ring file.
- You can delete Installation Manager installation kits from the repository. Perform this task using the administrative console graphical user interface. Open the administrative console and select **Jobs > Installation Manager installation kits**. For more information, see Installation Manager installation kits.
- You can submit a job to uninstall IBM Installation Manager. For example:
 - Using Jacl:

```
$AdminTask submitJob {-jobType uninstallIM -targetList {hostname} -jobParams { {installPath <IM install path>}}}
```

- Using Jython:

```
AdminTask.submitJob('-jobType uninstallIM -targetList [hostname] -jobParams [ [installPath <IM install path>] ]')
```

- You can submit a job to uninstall Installation Manager using the administrative console.
 1. In the administrative console, select **Jobs > Submit**.
 2. In the job type menu list, select **Uninstall IBM Installation Manager**. Click **Next**.
 3. Specify target names and target authentication.
 4. Specify the job parameters.
 - The following parameter is required: installPath, IBM Installation Manager installation location.
- You can submit a job to find Installation Manager data locations. You can add specific data locations, or search the system for Installation Manager data locations.
 1. In the administrative console, select **Jobs > Submit**.
 2. In the job type menu list, select **Add or search for Installation Manager data locations**. Click **Next**.
 3. Specify target names and target authentication.
 4. Specify the job parameters.
 - You can specify Installation Manager data locations.
 - You can search the system for Installation Manager data locations.

Results

You have installed, updated, or deleted Installation Manager and Installation Manager installation kits on a target machine.

What to do next

You can continue to view node resources and do other job management tasks such as submit jobs, create node groups for job submission, and view nodes.

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

APACHE INFORMATION. This information may include 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>.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Intellectual Property & Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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.

Trademarks and service marks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. For a current list of IBM trademarks, visit the IBM Copyright and trademark information Web site (www.ibm.com/legal/copytrade.shtml).

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

Index

A

- administrative agents
 - installation
 - planning 159
 - z/OS 437
- application server
 - install
 - environment 3
- automatic restart management (ARM) 421
 - activating 422
 - guidelines 423
 - installation
 - guidelines 423
 - status 423, 424

C

- cells
 - creating
 - network deployment 443
 - planning
 - network deployment 276
- configuration
 - differences 99
- customization
 - installation 431
- customization definitions
 - profile management tool 433
 - reviewing 433

D

- databases
 - scheduler 94
- deployment managers 438
 - creating
 - z/OS 437
 - planning 194
 - starting 420
- diagnostics
 - planning 425
- directory
 - installation
 - conventions 15
- DMZ Secure Proxy Server
 - installation
 - z/OS 37

F

- federated node
 - using 443
- federated server
 - stand-alone application servers
 - network deployment 264

- federated servers
 - network deployment
 - z/OS 442
- file systems
 - configuration 86

I

- installation
 - output destinations 93
 - planning 23
 - product 5
 - requirements
 - skills 18
 - z/OS 15, 16
 - stand-alone application server 117
 - verification tests 533, 534
 - z/OS 27, 33
- installation manager
 - z/OS 28
 - kit 28

J

- Java
 - installation
 - planning 70
- job managers
 - planning 324
 - submitting Installation Manager jobs 548

L

- language packs
 - installation
 - z/OS 539

N

- nodes
 - managed
 - planning 229
 - using 440
 - z/OS 440

P

- ports
 - default 111
- profile management tool (PMT)
 - preferences 430
 - starting 430
 - z/OS
 - administrative agents 445
 - stand-alone application servers 436

R

RACF

- installation
 - planning 72
- recovery
 - planning 420
- repositories
 - installation
 - z/OS 31
- requirements
 - installation
 - skills 18
 - z/OS 16
- Resource Recovery Service (RRS)
 - installation
 - planning 71

S

- secure proxy administrative agents
 - planning 388
- secure proxy servers
 - installation
 - planning 358
 - z/OS 445
- security
 - installation 113

U

- uninstallation
 - WebSphere Customization Toolbox
 - GUI 62
 - silently 63

W

- WebSphere Customization Toolbox
 - installation 44
 - GUI 45
 - silently 49
 - removing 44, 59
 - rolling back 44, 62
 - updating 61
 - using 43

Z

z/OS

- best practices 115
- customization variables 118, 160, 194, 229, 264, 277, 325
- customization worksheet 173, 180, 187, 207, 214, 221, 242, 249, 256, 269, 271, 273, 295, 304, 314, 400, 407, 413
- installation 5, 427
 - checklist 75
 - job managers 142, 151, 337, 344, 351
 - planning 18, 67, 68, 77, 111
 - web server plug-in 39
- JCL 83
- job managers 444
- logstreams 90
- naming conventions 99, 101, 107
- optional features 537
- planning
 - TCP/IP 73
- port conventions 95
- product considerations 82
- profile management tool 427, 429
- proxy servers 376, 382
- secure proxy servers 359, 370
- stand-alone application servers 133
- symbolic links 446
- terminology 78
- uninstallation 537, 545
- updating 537
- workload management (WLM) 99
- zpm 446, 448
 - administrative agents 498
 - deployment managers 461
 - federated servers 480
 - job managers 507
 - managed nodes 471
 - network deployment cells 484
 - secure proxy administrative agents 524
 - secure proxy servers 516
 - stand-alone application server 450