IBM Business Monitor
Version 8 Release 0

# *IBM Business Monitor Installation Guide*

# Contents


## Chapter 1. Installing IBM Business Monitor . . . . . 1

## Chapter 2. Planning to install IBM Business Monitor . . . . . 3

Choosing appropriate topologies. . . . . 3
Single-server topology . . . . . 3
High availability (network deployment) topology 3
Scalability . . . . . 4
Four-cluster topology . . . . . 7
Four-cluster topology with IBM Business Process Manager . . . . . 8
Using existing software prerequisites . . . . . 8
Profiles . . . . . 9
Choosing the profile type . . . . . 9
Stand-alone profiles . . . . . 10
Deployment manager profiles . . . . . 10
Custom profiles . . . . . 11
Database considerations . . . . . 11
MONITOR database considerations for DB2 . . 13
Cognos database considerations for DB2. . . . 14
MONITOR database considerations for DB2 for z/OS . . . . . 15
Cognos database considerations for DB2 for z/OS . . . . . 17
MONITOR database considerations for Oracle. . 18
Cognos database considerations for Oracle . . . 20
MONITOR database considerations for Microsoft SQL Server . . . . . 21
Cognos database considerations for Microsoft SQL Server . . . . . 23
User registry considerations . . . . . 23
Non-administrative user considerations . . . . . 24
Topology considerations . . . . . 24
Considerations for single-server topology . . . 24
Considerations for network deployment topology using deployment environment patterns. . . . 25
Considerations for custom network deployment topology . . . . . 26
Considerations for IBM Business Process Manager in a four-cluster topology environment . 26

## Chapter 3. Preparing to install. . . . . 29

Hardware and software requirements. . . . . 29
Preparing operating systems for product installation 29
Preparing AIX systems for installation . . . . 29
Preparing Linux systems for installation. . . . 30
Preparing Solaris systems for installation . . . 32
Preparing Windows systems for installation . . 33

## Chapter 4. Installing the IBM Business Monitor software . . . . . 35

Installing from the product launchpad . . . . . 35
Installing IBM Business Monitor interactively . . 37
Installing IBM Business Monitor silently. . . . . 40
Installing IBM Business Monitor silently using the command line . . . . . 40
Installing IBM Business Monitor silently using a response file . . . . . 45
Installing the information center . . . . . 46
Starting and stopping the local information center . . . . . 46
Updating the local information center . . . . 47

## Chapter 5. Creating the databases . . . 49

Creating or configuring database scripts using the database design tool . . . . . 50
Configuring MONITOR database scripts manually 51
Configuring COGNOSCS database scripts manually 54
Installing the MONITOR database manually . . . 55
Installing the COGNOSCS database manually . . . 56
Creating messaging engine tables manually . . . 57
Generating scripts for creating database objects in DB2 for z/OS. . . . . 58
Creating databases in the DB2 for z/OS subsystem 59
Setting up alias name definitions for connecting to the DB2 for z/OS server . . . . . 60
Creating DB2 for z/OS database objects using the createDB2.sh script . . . . . 61
Creating DB2 for z/OS database objects using the DB2 command line processor . . . . . 63
Considerations for HADR setup and configuration 64
Configuring Oracle Real Application Cluster (RAC) for use with IBM Business Monitor . . . . . 66
Configuring Oracle Data Guard for IBM Business Monitor . . . . . 67

## Chapter 6. Creating and augmenting profiles . . . . . 69

Creating and augmenting profiles using the Profile Management Tool . . . . . 69
Creating stand-alone profiles . . . . . 70
Creating deployment manager profiles . . . . 75
Augmenting deployment manager profiles . . . 80
Creating custom profiles for nodes . . . . . 84
Augmenting custom profiles for nodes . . . . 86
Creating and augmenting profiles using the manageprofiles command . . . . . 87

## Chapter 7. Verifying the installation . . 91

## Chapter 8. Determining port numbers 93

## Chapter 9. Configuring the environment 95

Creating the deployment environment using a pattern . . . . . 95
Importing deployment environment definitions based on design documents . . . . . 101


© Copyright IBM Corp. 2005, 2012

Adding an IBM Business Monitor deployment environment to an IBM Business Process Manager server deployment environment . . . 106
Installing IBM Business Process Manager widgets into IBM Business Monitor Business Space . . . . . 106
Installing IBM Business Monitor widgets into BPM Business Space . . . . . 107
Creating the deployment environment using custom topology . . . . . 107
Creating IBM Business Monitor clusters . . . 108
Adding cluster members . . . . . 109
Federating additional nodes . . . . . 109
Configuring CEI event services . . . . . 110
Configuring the environment using the configuration wizard . . . . . 110
Configuring the environment using wsadmin commands . . . . . 115
Configuring the environment manually. . . . . 117
Configuring the event emitter factory for IBM Business Monitor for z/OS . . . . . 117
Installing the IBM Business Monitor action services application . . . . . 118
Creating the Monitor action services group profile . . . . . 119
Installing Monitor scheduled services . . . 119
Creating and configuring a scheduler resource . . . . . 120
Installing dashboards for mobile devices . . 121
Installing event emitter services . . . . . 121
Creating resources for manually installed event emitter services . . . . . 121
Manually installing event emitter services 124
Using the configuration wizard to install event emitter services . . . . . 126

**Chapter 10. Configuring IBM Business Monitor components . . . . . 127**

Configuring IBM Cognos BI . . . . . 127
Configuring a new IBM Cognos BI service . . 127
Generating an EAR file for IBM Cognos BI on a custom IBM Business Monitor node . . 130
Configuring IBM Business Monitor and Business Space to use an existing IBM Cognos BI service . 131
Configuring IBM Cognos BI with WebSphere Portal . . . . . 133
Configuring the reporting data source in IBM Cognos BI . . . . . 134
Configuring IBM Business Monitor widgets for WebSphere Portal . . . . . 135
Configuring how to receive events . . . . . 135
Asynchronous event considerations . . . . . 135
Configuring authorization for asynchronous event delivery . . . . . 135
Receiving events from CEI . . . . . 136
Receiving events using table-based event delivery . . . . . 137
Configuring table-based event delivery in a single-cell environment . . . . . 137
Configuring table-based event delivery in a multiple-cell environment . . . . . 138
Receiving events using queue-based event delivery . . . . . 139
Configuring queue-based event delivery in a single-cell environment . . . . . 139
Configuring queue-based event delivery in a multiple-cell environment. . . . . 139
Configuring Business Space . . . . . 141
Configuring Business Space . . . . . 141
Configuring Business Space on a product profile using the Profile Management Tool. . 142
Creating Business Space profiles . . . . 144
Configuring Business Space as part of the Deployment Environment Configuration wizard . . . . . 182
Configuring Business Space for network deployment environments . . . . . 184
Configuring REST services . . . . . 184
Configuring Business Space and registering REST endpoints on the administrative console . . . . . 189
Configuring Business Space using the command line . . . . . 191
Creating a Business Space database design properties file . . . . . 193
Configuring the Business Space database 193
Registering Business Space widget REST service endpoints using the command line 195
Removing the virtual host from the primary cluster member. . . . . 196
Configuring a proxy server or load-balancing server to use with Business Space . . . . . 197
Enabling the Federation API across multiple deployment targets . . . . . 203
Enabling Business Space widgets for cross-cell environments . . . . . 204
Enabling Business Space widgets to work with multiple endpoints. . . . . 206
Configuring widgets for multiple products 210
Setting up specific widgets to work in Business Space . . . . . 211
Configuring the service monitor . . . . 211
Installing the default business space on z/OS . . . . . 212
Setting up security for Business Space . . . 214
Enabling security for Business Space . . 214
Selecting the user repository for Business Space . . . . . 216
Setting up SSO and SSL for Business Space . . . . . 219
Designating HTTP or HTTPS settings for Business Space . . . . . 220
Setting up security for system REST services . . . . . 220
Business Space widget security considerations . . . . . 221
Configuring Tivoli Access Manager WebSEAL to work with Business Space. . 221
Assigning the Business Space superuser role. . . . . 224

Assigning the Business Space superuser by user group . . . . . 226
Preventing users from creating business spaces . . . . . 228
Enabling searches for user registries without wildcards . . . . . 229
Commands (wsadmin scripting) for configuring Business Space . . . . . 230
addICMSystem command . . . . . 231
configureBusinessSpace command . . . 232
createBPMApiFederationDomain command . . . . . 235
deleteBPMApiFederationDomain command . . . . . 236
getBusinessSpaceDeployStatus command 237
installBusinessSpace command . . . . 238
installBusinessSpaceWidgets command 241
installHumanTaskManagementWidgets command . . . . . 242
listBPMApiFederationDomains command 243
modifyBPMApiFederationDomain command . . . . . 244
registerRESTServiceEndpoint command 245
removeICMSystem command . . . . . 247
showBPMApiFederationDomain command . . . . . 248
uninstallBusinessSpaceWidgets command 249
updateBusinessSpaceWidgets command 250
updateRESTGatewayService command 252
Updating Business Space templates and spaces after installing or updating widgets 253
Configuring the Business Space Ajax proxy 254
Adding proxy policies to the Business Space Ajax proxy . . . . . 255
Changing the timeout settings for the Business Space Ajax proxy . . . . . 255
Blocking IP addresses using the Business Space Ajax proxy . . . . . 256
Migrating Business Space (post-product migration) . . . . . 257
Configuring Business Space to work with Mashup Center . . . . . 257
Configuring widgets to work with WebSphere Portal . . . . . 259
Configuring SSO and SSL for widgets on WebSphere Portal . . . . . 263
updateEndpointBindingsOnPortal command . . . . . 264
Required entries for the proxy-config.xml file to configure widgets to work with WebSphere Portal . . . . . 265
Configuring Business Space to work with IBM Case Manager . . . . . 266
Configuring cross-cell security for IBM BPM and IBM Case Manager . . . . . 267
Registering IBM BPM widgets in IBM Case Manager . . . . . 270
Registering IBM Case Manager widgets in IBM Business Process Manager Advanced . 273
Registering IBM Case Manager REST services in IBM BPM . . . . . 273
Configuring the global process monitor model . . 276
Installing the global process monitor model manually . . . . . 277
Enabling events for the global process monitor model . . . . . 277
Configuring your dashboards for the global process monitor model . . . . . 278

**Chapter 11. Installing the showcase model. . . . . 281**

**Chapter 12. Updating IBM Business Monitor . . . . . 283**
Updating IBM Cognos BI . . . . . 283
Installing fix packs and interim fixes interactively 284
Installing fix packs silently . . . . . 286
Installing interim fixes silently. . . . . 287
Rolling back fix packs . . . . . 288
Uninstalling interim fixes interactively . . . . . 288
Uninstalling interim fixes silently. . . . . 289

**Chapter 13. Uninstalling IBM Business Monitor . . . . . 291**
Uninstalling IBM Business Monitor interactively 291
Uninstalling IBM Business Monitor silently . . . 292
Removing the showcase model . . . . . 293

# Chapter 1. Installing IBM Business Monitor

IBM® Business Monitor can be installed in multiple topologies. You can install all components on a single server, or you can distribute the components across multiple systems. To achieve a highly available environment with failover support, you can install IBM Business Monitor into a clustered environment that uses the clustering mechanism of WebSphere® Application Server or Process Server.

**Important:** IBM Business Monitor runs on multiple platforms. For details about supported operating systems, supported hardware, memory requirements, and disk space requirements, see the System requirements for IBM Business Monitor.

© Copyright IBM Corp. 2005, 2012

# Chapter 2. Planning to install IBM Business Monitor

IBM Business Monitor has multiple components that can be installed on a single server or across multiple servers in the network. During the installation process, there are many options to consider. When planning to install IBM Business Monitor, you must consider the available options and how you want to deploy the components in your network.

Information is provided to help you to determine which topology is most appropriate for your environment and to understand the options that are available during the installation.

Review the following information before beginning your IBM Business Monitor installation:

## Choosing appropriate topologies

IBM Business Monitor can be installed in many different configurations. A few basic topologies are provided. You might need to customize these to fit your environment.

To help you understand some of the possible installation deployments, the following topologies illustrate some common installations:

### Single-server topology

When you use the single-server topology, all supporting products and all IBM Business Monitor components are installed on the same physical server.

Installing IBM Business Monitor on a single server is ideal for development test environments, proof-of-concept environments, and simple deployments that do not require failover and high availability capabilities.

You can use the IBM Business Monitor installation program to install IBM Business Monitor and WebSphere Application Server. When you install IBM Business Monitor on a single server, the Cognos service is also installed. To view the monitored data, you can use either a business space or the portlet-based dashboards.

After you install IBM Business Monitor, create a stand-alone profile to define your runtime environment. All required IBM Business Monitor components are created when you create or augment a stand-alone profile.

### High availability (network deployment) topology

IBM Business Monitor uses the high availability capabilities in WebSphere Application Server or Process Server Network Deployment (ND) environments. Network deployment provides the capacity, scalability, and robustness that is generally required of a production environment. In network deployment environments, a group of servers can be used collaboratively to provide workload balancing and failover. The servers are managed centrally, using a single administrative console.

IBM Business Monitor uses the same architecture model as WebSphere Application Server or Process Server. Using this model, you create environments that have cells, nodes, servers, and optionally clusters.

If you choose one of the available deployment environment patterns (single cluster or four-cluster), the deployment environment wizard helps you to configure the clusters, servers, and components that you need.

© Copyright IBM Corp. 2005, 2012

The cell is the main administrative domain. You can think of a cell as a logical grouping of servers, clusters, or a combination of both. (A cluster is a group of application servers that collaborate for the purposes of workload balancing and failover.) Using servers and clusters, you can install IBM Business Monitor into a single cell that is both highly available and scalable.

A managed node (a node within a cell) contains one or more servers. Each server provides a runtime environment. Managed servers are created within a managed node, which has been defined by a custom profile. Each of the managed nodes is federated to the same deployment manager, and the deployment manager manages all managed nodes in the cell. Servers can be grouped into clusters, which are also managed by the deployment manager. For a network deployment environment, you should cluster your applications so that the applications are protected from the failure of a single server (high availability), the workload of the applications is spread across a number of equivalent servers (workload balancing), or both.

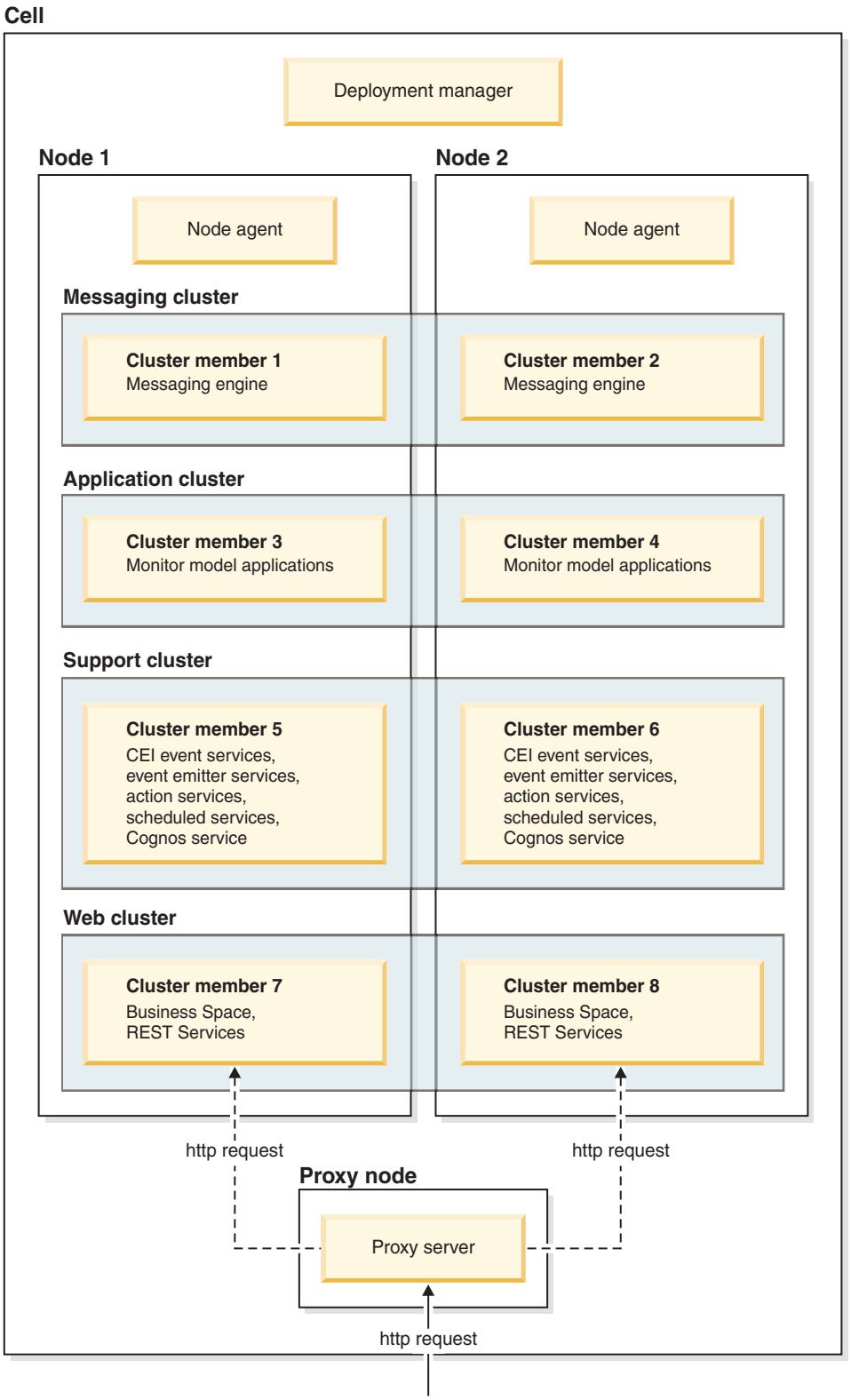
For more information on high availability, see "High availability and workload sharing" in the related links.

In an ND environment, you will normally set up a proxy server or an HTTP server for security reasons and for workload balancing. See the "Scalability" topic for more information about the proxy server.

## Scalability

Installing IBM Business Monitor components and monitor models to a cluster enhances your ability to manage their workload. Distributing the components and monitor models across multiple clusters, grouping components based on common resource usage patterns, enables you to manage the individual workload of each cluster based on the resource usage pattern of the installed components. See the "Four-cluster topology" topic for a suggested starting point when planning for a scalable topology.

The following diagram shows a cell with two managed nodes.




## Messaging engines

When deployed to a cluster, the messaging engine created for the IBM Business Monitor service integration bus is only active on one cluster member at a time. This behavior is specified by the default service integration bus policy. While the default service integration bus policy can be customized, the

policy must always be of type "One-of-N." A "One-of-N" policy allows only one instance of the messaging engine to become active in a cluster, providing high availability (protecting components and models from the failure of a single server), but not scalability (the ability to expand as resources are added).

You can minimize use of the messaging engine and enable better performance by using the feature that allows the common event infrastructure (CEI) event service to bypass the use of Java Messaging Service (JMS) queues and directly submit events into the IBM Business Monitor database. See "Receiving events using table-based event delivery" in the related task links for more information.

### Support components

Support components include the CEI event service, IBM Cognos® Business Intelligence service, action services, event emitter services, and scheduled services. Except for the scheduled services, add new cluster members for increased capacity.

Most of the workload for the scheduled services occurs on the database server. As the workload of the scheduled services increases, you should monitor, evaluate, and tune the database server as needed. The workload of the scheduled services can also be managed by either enabling or disabling the various scheduled services or by editing the service intervals associated with each scheduled service. See "Managing Monitor scheduled services" in the related tasks links for more information.

### Web components

Web components include Business Space, widgets, and the IBM Business Monitor REST API service. Add new cluster members for increased capacity.

In an ND environment, you will normally set up a proxy server or an HTTP server for security reasons and for workload balancing. Instead of incoming HTTP requests going directly to a WebSphere Application Server, they go to a proxy server that can spread the requests across multiple application servers that perform the work. Create a proxy server in WebSphere Application Server. You can use other routing servers in place of or in front of the proxy server, for example IBM HTTP Server. The benefit of using the proxy server is that it is integrated with WebSphere Application Server and therefore easy to use and maintain.

**Important:** The proxy server (or an alternate routing server) is required for workload balancing HTTP requests across two or more cluster members. The proxy server allows clients to access the applications within this topology.

### Monitor model applications

Monitor model applications are packaged as standard Java enterprise application archives (EARs). The monitor model application scales with the number of cluster members in the cluster.

### Memory considerations

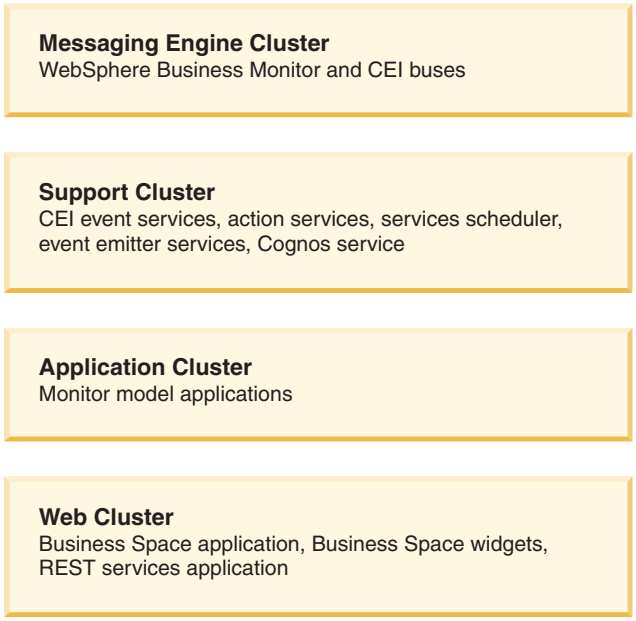
The amount of memory available to a single cluster member depends on the address space layout of the operating system and on whether the JVM that runs it is a 32-bit or 64-bit process. While a 64-bit JVM can access anywhere from 500 GB to 4 GB of memory, a 32-bit JVM might only have access to as little as 2 GB of memory (for example on 32-bit Windows).

As a general guideline, consider adding a second cluster for deploying monitor model applications when deploying more than ten monitor model applications if the cluster members are running on a 32-bit JVM. This is a guideline only, as individual workloads and models vary.

## Four-cluster topology

You can install IBM Business Monitor into many topologies. You can use the four-cluster topology to set up a high performance environment.

The following four-cluster topology uses the Remote Messaging, Remote Support, and web deployment environment pattern. This pattern groups the IBM Business Monitor applications into four clusters in a single cell.




**Messaging engine cluster**

- Messaging engine for the IBM Business Monitor bus
- Messaging engine for the common event infrastructure (CEI) bus

**Support cluster**

- CEI event service
- Event emitter services
- Action services
- Monitor scheduled services
- IBM Cognos Business Intelligence service

**Application cluster**

- Monitor model applications

**Web cluster**

- Business Space application
- Business Space widgets
- Representational State Transfer (REST) services application

**Note:** For improved performance, place the event emitter services and CEI event service on the same cluster. Event emitter services includes both the REST event emitter and the JMS event emitter.

**Related tasks**:

"Considerations for IBM Business Process Manager in a four-cluster topology environment" on page 26
You can configure a Four cluster topology with IBM Business Process manager to create a combined IBM® Business Process Manager and IBM Business Monitor deployment environment using the Remote Messaging, Remote Support, and Web (four-cluster) pattern. Because one IBM Business Monitor deployment environment can monitor all applications in the cell, you should only create one IBM Business Monitor deployment environment in a given cell. The four-cluster topology combines IBM Business Monitor and IBM Business Process Manager messaging engine clusters into a single cluster.

### Four-cluster topology with IBM Business Process Manager

You can create a combined IBM Business Process Manager and IBM Business Monitor deployment environment using the Remote Messaging, Remote Support, and Web (four-cluster) pattern. Because one IBM Business Monitor deployment environment can monitor all applications in the cell, you should only create one IBM Business Monitor deployment environment in a given cell.

The four-cluster topology combines IBM Business Monitor and IBM Business Process Manager messaging engine clusters into a single cluster. The following four-cluster topology uses the Remote Messaging, Remote Support, and web deployment environment pattern.

**Messaging engine cluster**

Messaging engine for the IBM Business Monitor bus

Messaging engine for the common event infrastructure (CEI) bus

Messaging engine for the Process Server bus

Messaging engine for the Performance Data Warehouse bus

(BPM Advanced only) Messaging engine for the Service Component Architecture (SCA) bus

(BPM Advanced only) Messaging engine for the Business Process Execution Language (BPEL) bus

**Support cluster**

CEI event service

Event emitter services

Action services

Monitor scheduled services

IBM Cognos Business Intelligence service

Performance Data Warehouse

(BPM Advanced only) Business rules manager

**Application cluster**

Monitor model applications

Process applications

(BPM Advanced only) BPEL applications

**Web cluster**

Business Space application

Business Space widgets

Representational State Transfer (REST) services application

(BPM Advanced only) Business Process Choreographer tools

## Using existing software prerequisites

You can install IBM Business Monitor on servers where the prerequisite software is installed.

### Existing application servers

You can install the IBM Business Monitor server on a physical server where an application server platform is currently installed. The following application server platforms for IBM Business Monitor are supported:

- WebSphere Application Server
- Process Server
- WebSphere Enterprise Service Bus

You can augment an existing profile, or you can create a new profile to contain the IBM Business Monitor server.

### Existing WebSphere Portal

IBM Business Monitor no longer provides portlet-based dashboards. However, your IBM Business Monitor widgets can still be displayed in WebSphere Portal. See the related task link for information.

## Profiles

A profile defines the runtime environment and includes all of the files that the server processes in the runtime environment. In a high availability environment, you need multiple profiles to appropriately manage the complexity of the system. You can either create new profiles or augment existing profiles.

IBM Business Monitor has profile templates to enable functionality that is specific to IBM Business Monitor. After installing the product, you can create and augment profiles either using the Profile Management Tool wizard (in the WebSphere Customization Toolbox) or with the **manageprofiles** command. (If you are running Solaris in 64-bit mode, you must use the **manageprofiles** command.)

The IBM Business Monitor profile types are an extension of the similarly named profile types provided by WebSphere Application Server. The profile types provided by IBM Business Monitor are not the same as the profile types provided by WebSphere Application Server.

Using new profiles is more efficient and less prone to error than installing the product multiple times. Developers can use separate profiles for development and testing. By using profiles rather than multiple product installations, you gain the following advantages:

- You need to maintain only a single set of core product files.
- You save disk space.
- You can update the product more easily.

## Choosing the profile type

A profile defines a unique runtime environment, with separate command files, configuration files, and log files. Profiles define three different types of environments: stand-alone single server, deployment manager, and managed node. Using profiles, you can have more than one runtime environment on a system, without having to install multiple copies of the product.

For a single-server environment, create a stand-alone profile.

For a network deployment environment, complete the following steps:

1. Create the deployment manager profile before creating the other profiles. If you created a deployment manager profile before installing IBM Business Monitor (for example, for WebSphere Application Server or Process Server) and you plan to use the same deployment manager profile to manage IBM Business Monitor nodes, augment the profile using the template that IBM Business Monitor provides.

2. Create a custom profile for each node that you plan to add to the server cluster. Alternatively, augment an existing custom profile for each node that you plan to add.

   **Note:** If the database server contains multiple versions of DB2® installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

Templates for each profile are located in the `app_server_root/profileTemplates` directory. The following profile templates are available:

| Profile | When to use |
|---|---|
| Stand-alone monitor server | For IBM Business Monitor single-server environments. |
| Monitor server deployment manager | If you are setting up a network deployment environment, create or augment this profile first. If you have created a deployment manager before installing IBM Business Monitor and you plan to use the same deployment manager profile to manage IBM Business Monitor nodes, augment the profile using the template provided by IBM Business Monitor. |
| Monitor server custom profile | If you are setting up a network deployment environment, create or augment custom nodes and later use the administrative console to install specific applications to the various custom nodes. |

## Stand-alone profiles

For IBM Business Monitor, use a stand-alone profile, also known as a stand-alone application server profile, for single-server environments.

Each stand-alone application server node has its own administrative console, which you use to manage the node. A stand-alone node can include more than one server.

A stand-alone server is easy to set up, and has a First steps console from which you can start and stop the server and install the Showcase sample. If you install the sample to the stand-alone server, you can explore the resources used for the sample in the administrative console.

You can deploy your own solutions to a stand-alone server, but a stand-alone server cannot provide the capacity, scalability, or robustness that is generally required of a production environment. For your production environment, it is better to use a network deployment environment.

## Deployment manager profiles

A deployment manager is a server that manages operations for a logical group, or cell, of other servers. In network deployment environments, a group of servers are used collaboratively to provide workload balancing and failover. The deployment manager is the central location for administering the servers and clusters in the cell.

To create a deployment environment, the deployment manager profile is the first profile that you create or augment. . The deployment manager has a First steps console, from which you can start and stop the deployment manager and start its administrative console. You use the administrative console of the deployment manager to manage the servers and clusters in the cell. This includes configuring servers and clusters, adding servers to clusters, starting and stopping servers and clusters, and deploying modules to them.

Although the deployment manager is a type of server, you cannot deploy modules to the deployment manager itself.

After creating or augmenting the deployment manager for IBM Business Monitor in a network deployment environment, you can then create or augment custom nodes and federate them into, or make them a part of, the deployment manager to create a cell, a group of nodes or clusters that are centrally administered.

Create or augment the deployment manager profile before creating or augmenting the custom profiles. If you created a deployment manager profile before installing IBM Business Monitor and you plan to use the same deployment manager profile to manage IBM Business Monitor nodes, augment the profile using the template provided by IBM Business Monitor.

### Custom profiles

To configure a network deployment environment for IBM Business Monitor, create custom nodes and federate them into, or make them part of, the deployment manager cell that will manage them. Alternatively, you can augment an existing custom profile for each node that you plan to add to the cell. You can later use the administrative console to install specific applications to the various custom nodes.

A custom profile is an empty node that does not include the default applications or server that a stand-alone server profile includes. During the process of creating or augmenting a custom profile, you federate the node to identify the deployment manager profile that you plan to use to manage the node. After the custom profile has been federated to the deployment manager, the node becomes a *managed node*.

A managed node contains a node agent and can contain managed servers. In a managed node, you can configure and run managed servers. The servers that are configured on a managed node make up the resources of your deployment environment. These servers are created, configured, started, stopped, managed, and deleted using the administrative console of the deployment manager. Processes on the managed node can include cluster members that the deployment manager uses to balance the workload for heavily used applications.

A managed node can contain one or more servers, which are managed by a deployment manager. You can deploy solutions to the servers in a managed node, but the managed node does not have its own administrative console. The managed node is defined by a custom profile and has a First steps console.

## Database considerations

The main MONITOR database stores the IBM Business Monitor configuration, monitor model metadata, and monitored data. The IBM Cognos Business Intelligence configuration is stored in a separate IBM Cognos BI content store database named COGNOSCS. Profile creation assumes that both the MONITOR and COGNOSCS database are created in the same database instance.

You can use a common database user name for the MONITOR and COGNOSCS databases. However, you might want to use separate names because IBM Cognos BI creates its own content store tables in the schema of the provided database name when IBM Cognos BI first starts.

The MONITOR database is also used to store schemas for the following components during stand-alone profile creation:

- Business Space
- Common event infrastructure (CEI) messaging engine message store
- IBM Business Monitor messaging engine message store

If you are not using a stand-alone profile, you can use the same database or different databases for these components, and additionally for the CEI data store, which is not required and therefore is not created or enabled by default.

For production environments, you can choose from the following supported database products:

- DB2
- DB2 for z/OS®
- Oracle
- Microsoft SQL Server

Multiple types of data are stored in the MONITOR database. When you create the IBM Business Monitor profile or run the database scripts, you create database tables that contain configuration data for IBM Business Monitor. Later, when each monitor model is installed, additional tables are created to store data for that monitor model. When events are processed, monitor model instance data is stored in these tables. The dashboards then refer to these tables.

**Tip:** In a network deployment environment, create the MONITOR and COGNOSCS databases before starting the deployment manager and creating other custom profiles.

**Tip:** If the COGNOSCS database is remote from the IBM Cognos BI server, you must install a database client on the IBM Cognos BI server machine. See the details in the database-specific database consideration topics.

## Creating the databases

There are several ways to create the MONITOR and COGNOSCS databases.

- If the database software is installed on the same server as IBM Business Monitor, you can have the Profile Management Tool or the manageprofiles command create local databases when the profile is created.

  **Note:**
  - For DB2, the user who creates the profile must have credentials to create the database.
  - For Oracle or SQL Server, a database administrator user ID and password must be provided to the Profile Management Tool or manageprofiles command so that database objects can be created in an existing database instance.
- You can have the profile management function generate database scripts, using the configuration values that were selected when the profile was created. Select the profile creation option to delay execution of database scripts and, at a later time, run the generated scripts to create the database objects on the database server.
- You can manually create the database using scripts provided on the installation media or in the IBM Business Monitor installation dbscripts directory. Variables in the scripts can be configured manually or by using the database design tool (DbDesignGenerator).

  **Important:** Use this option with DB2 for z/OS.

In the MONITOR database, if you rename the table spaces for example data, then when you are creating the schema for monitor models, you must export the create schema scripts and change the table space names to match the names that were used during initial database creation.

## Database size

The IBM Business Monitor database scripts for the MONITOR database create multiple table spaces to store data. The table space names and configuration can be altered depending on the enterprise standards and performance and sizing requirements. For development and test installations with minimal amounts of data, 1 GB of database storage should be sufficient. For production environments, size the database based on the amount of data that you intend to monitor.

### Securing the databases

When the databases are created, the runtime database user is granted privileges to administer database objects by default, which simplifies the creation of the databases and enables the IBM Business Monitor server to automatically manage the monitor model database schema when models are deployed and removed. If you must secure the databases, see Securing the MONITOR database environment and Configuring IBM Cognos BI security.

## MONITOR database considerations for DB2

There are specific recommendations for databases that are hosted on DB2.

### Globalization considerations

DB2 must be installed using the UTF-8 Universal character set. Using this character set ensures that monitor model metadata and instance data containing native language characters can be saved to the database. Additionally, IBM Cognos Business Intelligence requires a UTF-8 database. The `createDatabase.sql` script creates the database as UTF-8 automatically.

The `createDatabase.sql` script creates the databases with the following default territory setting:

```
TERRITORY EN_US
```

To change the default language, change the TERRITORY to a supported territory setting from the DB2 Supported territory codes and code pages. Territory settings must use the UTF-8 code set. For example, to change the territory to French, you would use:

```
TERRITORY FR_FR
```

### DB2 Express Edition considerations

DB2 Express Edition can use a maximum of 4 GB of instance memory, even if the system has more than 4 GB of memory. For more information about which version of DB2 to use, see the related reference links.

Currently, there is a known limitation in DB2 Express installer related to the inclusion of national language (NL) strings in properties passed to it from the IBM Business Monitor installer. The following values, which are passed to DB2 Express when it is being installed cannot have NL strings in them:

Linux Windows

- Linux Instance user name and password: `bpminst`
- Linux Fenced user name and password: `bpmfenc`
- Linux Administration server (DAS) user name: `bpmadmin`
- Windows Administrative user name: `bpmadmin`

### DB2 catalog requirements

If the DB2 database is remote from the IBM Cognos BI server, then the MONITOR database must be cataloged by the DB2 client installed with the IBM Cognos BI server.

**Important:** Make sure that the alias name on the remote IBM Cognos BI server is the same as the cataloged database name of the MONITOR database. Otherwise cube creation will fail when a monitor model is deployed.

See the IBM Cognos BI database considerations topic for complete details.

### MONITOR database security considerations

When you are using the Profile Management Tool (in the WebSphere Customization Toolbox) or the manageprofiles command to create the DB2 database, the administrative user creating the profile also attempts to create the database. The IBM Business Monitor runtime database user (@DB_USER@) that is specified during profile creation must already exist in the operating system.

By default, the IBM Business Monitor runtime database user is granted DBADM (database administrator) privileges as part of the database creation. This enables the IBM Business Monitor server to automatically manage the monitor model database schema when models are deployed and removed. To secure the database, you can create the database manually and grant the runtime database user only the privileges required for runtime operations. See "Installing the MONITOR database manually" on page 55 and Securing the Monitor database environment.

### DB2 locking considerations

When there are a large number of events, the MONITOR database can deadlock on two or more different transactions waiting for the same database lock. When this happens, one of the transactions fails and is retried.

To eliminate deadlocks on DB2 LUW while maintaining concurrent processing under high volume, enter the following in the DB2 command window:

```
db2set DB2_SKIPINSERTED=ON
db2set DB2_SKIPDELETED =ON
```

Multiple threads will not deadlock when the DB2 instance registry variables DB2_SKIPINSERTED and DB2_SKIPDELETED are set to **ON**.

### Health Monitor considerations

If you are using DB2 Health Monitor (Automatic Maintenance), exclude the SIBOWNER from the automatic statistics collection. For more information, see the technote in related reference.

## Cognos database considerations for DB2

IBM Cognos Business Intelligence uses the COGNOSCS (IBM Cognos BI content store) database for configuration and report specification information, and uses the MONITOR database for actual reporting data.

### COGNOSCS database considerations for IBM Cognos BI

The IBM Cognos BI service creates tables in the IBM Cognos BI content store database the first time it is started. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

The COGNOSCS database must be used only for IBM Business Monitor data. You must not add data directly to the COGNOSCS database, or use the database with other databases to create reports against such data (combined or not with data created in IBM Business Monitor).

### MONITOR database considerations for IBM Cognos BI

If your MONITOR database is remote from the server or cluster that the IBM Cognos BI service is deployed on, you must install a full database client such as the IBM Data Server Client on the IBM Cognos BI server to deploy cubes.

The remote database must be cataloged before you can publish IBM Cognos BI cube packages during monitor model deployment. The cataloged name must be the database name that you entered for the MONITOR database. Otherwise, you must change the WBMONITOR_DB data source in IBM Cognos BI to point to the correct cataloged name.

IBM Cognos BI needs access to DB2 client commands when publishing cube packages during model deployment.

- Windows The DB2 client must be in the server PATH.
- Linux UNIX The correct environment variables must be set for the DB2 user starting the IBM Business Monitor server.

### 32-bit client requirement

The database client that IBM Cognos BI uses to connect to the MONITOR database must be a 32-bit client. On a Windows system, DB2 makes available both 64-bit and 32-bit libraries without additional configuration. On a non-Windows system, IBM Cognos BI requires access to the following 32-bit DB2 libraries:

- Libraries in the `/lib` directory of the DB2 server install (for example, `/opt/ibm/db2/V9.7/lib32`)
- Libraries in the `/lib` directory in the instance directory (for example, `/home/db2inst1/sqllib/lib32`)

If you are using 64-bit DB2 and are not using Windows, complete the following steps to configure a path to the DB2 32-bit libraries:

1. In the administrative console, click **Servers** > **Server types** > **WebSphere application servers** > ***server_name***. The Configuration panel is displayed.
2. Under **Server Infrastructure**, expand **Java and Process Management** and click **Process Definition**.
3. Under Additional Properties, click **Environment Entries**. Add the path to the 32-bit libraries as described below:
   - Windows No change required.
   - Linux UNIX Add the path to the DB2 32-bit server libraries to the following environment variable using a ":" as a delimiter.

     For Linux and Solaris: LD_LIBRARY_PATH

     For AIX: LIBPATH

## MONITOR database considerations for DB2 for z/OS

There are specific recommendations for databases that are hosted on DB2 for z/OS. A dedicated storage group (STOGROUP) is recommended for IBM Business Monitor. The storage group must be created before the MONITOR database is created.

### Globalization considerations

DB2 for z/OS must be installed using the UTF-8 Universal character set. Using this character set ensures that monitor model metadata and instance data containing native language characters can be saved to the database. The `createDatabase_Monitor.sql` and `createTablespace_Monitor.sql` scripts create the database as UTF-8 automatically.

The DIM_TIME table contains a column for populating dashboard reports with a translated month name. The location settings in z/OS are not used for creating the month names. There is an SQL statement in the `createTable_Monitor.sql` file that you can use to override the month name entries and define your own month names.

## General database considerations

DB2 for z/OS requires the addition of two bufferpools. The following 32K bufferpools need to be created by the database administrator before running the database scripts:

- BP32K
- TMPBP32

DB2 for z/OS requires a TEMP database for storing declared temporary tables.

- Create a dedicated STOGROUP to contain the IBM Business Monitor data.
- Create a TEMP database and a TEMP table space to contain the declared temporary tables for processing scrollable cursors. Examples are shown below.

  **For DB2 for z/OS version 8**, a temp database and table space must be created if it does not already exist. The following is an representative example of a TEMP database definition:

  ```
  CREATE DATABASE TEMP AS TEMP STOGROUP SYSDEFLT;
  CREATE TABLESPACE TEMP IN TEMP
  USING STOGROUP SYSDEFLT
  BUFFERPOOL BP32K
  SEGSIZE 32;
  ```

  **For DB2 for z/OS version 9 and version 10 in a non-data-sharing environment**, the TEMP database is DSNDB07 and is created during database installation. Temporary table spaces are added to the existing TEMP database. The following is a representative example of a temporary table space:

  ```
  CREATE TABLESPACE WBITEMP IN DSNDB07
  USING STOGROUP SYSDEFLT
  BUFFERPOOL BP32K
  SEGSIZE 32;
  ```

  **For DB2 for z/OS version 9 and version 10 in a data-sharing environment**, a WORKFILE database must be created. Only one WORKFILE database can be created per subsystem. The following is a representative example for creating a WORKFILE database and temporary table space:

  ```
  CREATE DATABASE WORKTEMP AS WORKFILE STOGROUP SYSDEFLT;
  CREATE TABLESPACE WBITEMP IN WORKTEMP
  USING STOGROUP SYSDEFLT
  BUFFERPOOL BP32K
  SEGSIZE 32;
  ```

For detailed information about how the TEMP database and TEMP table spaces are set up, refer to DB2 for z/OS information center. See the related link.

**Note:** If you are using DB2 for z/OS and you intend to use SPUFI for running the database scripts, use FTP to transfer the files to the z/OS database server. The IBM Business Monitor database scripts end with a line-feed character. The FTP server on z/OS will correctly map the line feed to an end-of-line character for the database script.

DB2 for z/OS version 8 also requires work file database storage for SQL statements that require working storage, such as sorts. This requires the addition of a table space to support sorting operations in addition to the TEMP database for version 8. In DB2 for z/OS version 9 and 10, the work file database and TEMP databases are combined. See the DB2 for z/OS information center for the procedures and sizing recommendations for creating work file databases.

Set the **RRULOCK** subsystem parameter to **YES** for greater concurrency.

If data movement service is to be enabled, increase the number of locks per user, NUMLKUS, to at least 100,000.

### JDBC driver

IBM Business Monitor uses the JDBC 4.0 driver. By default, the Profile Management Tool points to the `db2jcc4.jar` file supplied in **app_server_root\jdbcdrivers\DB2**. For DB2 for z/OS installations, it is recommended that you use the JDBC 3.0 driver `db2jcc.jar` that is shipped with DB2.

### Database substitution variables

Monitor model schema generation for DB2 for z/OS requires the database name and storage group variables to be provided. To minimize the manual substitution of variables, the following file is created when you create a profile:

`profile_root/properties/monitor_database.properties`

This file contains the following properties:

```
databaseName
db2zOSStorageGroup
```

Set the **databaseName** to the database name used in the Profile Management Tool or **manageprofiles** command for creating the database. Set the **db2zOSStorageGroup** to the DB2 storage group for the MONITOR database. If the variable names are left empty, the values are not substituted for the variables in the create schema scripts for the monitor models.

## Cognos database considerations for DB2 for z/OS

IBM Cognos Business Intelligence uses the COGNOSCS (IBM Cognos BI content store) database for configuration and report specification information, and uses the MONITOR database for actual reporting data.

### COGNOSCS database considerations for IBM Cognos BI

The IBM Cognos BI service creates tables in the IBM Cognos BI content store database the first time it is started. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

The COGNOSCS database must be used only for IBM Business Monitor data. You must not add data directly to the COGNOSCS database, or use the database with other databases to create reports against such data (combined or not with data created in IBM Business Monitor).

For DB2 on z/OS, you must manually create the database and table spaces. Update the table create scripts used by DB2 during startup with the database and table space names used when they were created.

### MONITOR database considerations for IBM Cognos BI

If your MONITOR database is remote from the server or cluster that the IBM Cognos BI service is deployed on, you must install a full database client such as DB2 Connect on the IBM Cognos BI server to deploy cubes.

The remote database must be cataloged before you can publish IBM Cognos BI cube packages during monitor model deployment. The cataloged name must be the database name that you entered for the MONITOR database. Otherwise, you must change the WBMONITOR_DB data source in IBM Cognos BI to point to the correct cataloged name.

IBM Cognos BI needs access to DB Connect client commands when publishing cube packages during model deployment.

- Windows The DB2 Connect client must be in the server PATH.
- Linux UNIX The correct environment variables must be set for the DB2 user starting the IBM Business Monitor server.

### 32-bit client requirement

The database client that IBM Cognos BI uses to connect to the MONITOR database must be a 32-bit client. On a Windows system, DB2 Connect makes available both 64-bit and 32-bit libraries without additional configuration. On a non-Windows system, IBM Cognos BI requires access to the following 32-bit DB2 Connect libraries:

- Libraries in the `/lib` directory of the DB2 Connect server install (for example, `/opt/ibm/db2/V9.7/lib32`)
- Libraries in the `/lib` directory in the instance directory (for example, `/home/db2inst1/sqllib/lib32`)

If you are using 64-bit DB2 Connect and are not using Windows, complete the following steps to configure a path to the DB2 Connect 32-bit libraries:

1. In the administrative console, click **Servers** > **Server types** > **WebSphere application servers** > ***server_name***. The Configuration panel is displayed.
2. Under **Server Infrastructure**, expand **Java and Process Management** and click **Process Definition**.
3. Under Additional Properties, click **Environment Entries**. Add the path to the 32-bit libraries as described below:
   - Windows No change required.
   - Linux UNIX Add the path to the DB2 Connect 32-bit server libraries to the following environment variable using a ":" as a delimiter.

     For Linux and Solaris: LD_LIBRARY_PATH

     For AIX: LIBPATH

## MONITOR database considerations for Oracle

There are specific recommendations for databases that are hosted on Oracle.

### Globalization considerations

Oracle must be installed using the UTF-8 Universal character set (AL32UTF8) instead of the default database character set (WE8ISO8859P1 - ISO 8859-1 West European). Using this character set ensures that monitor model metadata and instance data containing native language characters can be saved to the database. Additionally, IBM Cognos BI requires a UTF-8 database.

Oracle manages the language and locale settings with two database parameters:

NLS_LANGUAGE

NLS_TERRITORY

To change the default language for the databases, change the NLS_LANGUAGE parameter to a supported language for Oracle. Territory settings define the defaults for data formatting, currency, and so on. Set the NLS_TERRITORY parameter to change the Oracle instance.

The DIM_TIME table contains a column for populating dashboard reports containing time dimensions with a translated month name. By default, the locale code for the NLS_LANGUAGE setting is used for populating the DIM_TIME table entries. To change the default language, change the NLS_LANGUAGE for the Oracle instance or for the current session before running the `createTables.sql` script. There is also an SQL statement in `createTables.sql` that you can use to override the month name entries and define your own month names.

## MONITOR security considerations

When you are using the Profile Management Tool (in the WebSphere Customization Toolbox) or the manageprofiles command to create the Oracle database objects, the database administrative user specified in the profile creation creates the database objects and a MONITOR schema. On Oracle, a schema is both a collection of database objects and a user ID that can log into the database.

By default, the MONITOR schema owner is also the runtime database user, and is granted privileges to create other schemas and database objects as part of the database creation. This enables the IBM Business Monitor server to automatically manage the monitor model database schema when models are deployed and removed. To secure the database, you can create the database manually. The MONITOR schema owner, or a different user, can be used as the IBM Business Monitor runtime database user. In a secured environment, you can grant the runtime database user only the privileges required for runtime operations. See the topics "Installing the database manually" and "Securing the MONITOR database environment" in the related links.

## JDBC driver

JDBC support is provided by the Oracle JDBC drivers for JVM 1.6. The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.

By default, the Profile Management Tool points to the `ojdbc6.jar` file supplied in **app_server_root\jdbcdrivers\Oracle**. Alternatively, you can download another Oracle `ojdbc6.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command.

## XA recovery

You must apply special grants for Oracle's XA recovery to work correctly. Run the following commands as user SYS:

```
grant select on pending_trans$ to <user>;
grant select on dba_2pc_pending to <user>;
grant select on dba_pending_transactions to <user>;
grant execute on dbms_system to <user>;
```

where **<*user*>** is the user name for the MONITOR database that is configured during profile creation.

## Materialized Views

Dashboard page loading performance can degrade as you build up large volumes of monitoring data in your database. After you have more than approximately 10 million monitoring context instances, you might want to enable your database vendor's option to precompute the data.

When using DB2 you can enable materialized query tables (MQTs) to improve query performance, as described in “Managing the cube summary table refresh.” When using Oracle, you can use materialized views for the same purpose.

Like an MQT on DB2, a materialized view can precompute the values of key performance indicators (KPIs) and of IBM Cognos BI cube measures on Oracle. When the dashboard requests the value, the precomputed value is returned almost immediately, instead of the aggregation, such as an average, being computed against every monitoring context instance.

To define a materialized view, the Oracle database administrator (DBA) specifies the following settings:

**ON COMMIT**
Automatically refreshes the materialized view whenever a transaction that changes data in the table is committed (that is, when the data movement services runs).

**FAST** Incrementally updates data during a refresh.

You can find an example script that defines a FAST, ON COMMIT materialized view for the Showcase (Better Lender) sample in the following directory: **app_server_root\installableApps.wbm\showcase\OracleMaterializedViews_Sample**.

# Cognos database considerations for Oracle

IBM Cognos Business Intelligence uses the COGNOSCS (IBM Cognos BI content store) database for configuration and report specification information, and uses the MONITOR database for actual reporting data.

## COGNOSCS database considerations for IBM Cognos BI

The IBM Cognos BI service creates tables in the IBM Cognos BI content store database the first time it is started. The database user provided for accessing the IBM Cognos BI content store database must have full access to Oracle to create tables, views, sequences, triggers, and so on. In IBM Cognos BI, you cannot specify a separate schema name; the IBM Cognos BI objects are created in the default schema and default table space of the database user. It is recommended that you create a new database user for the content store database only.

**Important:** Do not use the SYSTEM user for this purpose, because you do not want the IBM Cognos BI database objects to be created in the system area.

The COGNOSCS database must be used only for IBM Business Monitor data. You must not add data directly to the COGNOSCS database, or use the database with other databases to create reports against such data (combined or not with data created in IBM Business Monitor).

## MONITOR database considerations for IBM Cognos BI

If your MONITOR database is remote from the server or cluster that the IBM Cognos Business Intelligence service is deployed on, you must install a full database client or the Oracle Instant Client on the IBM Cognos BI server to deploy cubes.

The Oracle instance for IBM Cognos BI must be addressable by a TNSNAMES entry in the Oracle client on the IBM Cognos BI server. The entry in TNSNAMES must use the same name as the database instance name that you entered for the MONITOR database during profile creation (for example, ORCL). Otherwise, you must to change the WBMONITOR_DB data source in IBM Cognos BI to point to the correct TNSNAMES entry.

If you are using Oracle Instant Client, the path to the client must be in the system path. A `TNSNAMES.ORA` file must also be included with an entry for the Oracle database server, and the TNS_ADMIN environment variable must be set to point to the directory containing the `TNSNAMES.ORA` file.

**Important:** Install the SQLPlus command utility with Oracle Instant Client for troubleshooting purposes.

The following example shows the contents of a valid `TNSNAMES.ORA` file. (The uppercase ORCL is the alias for the database connection.)

```
ORCL =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
(CONNECT_DATA =
```

```
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

IBM Cognos BI needs access to Oracle client commands when publishing cube packages during model deployment.

- Windows The Oracle client must be in the server PATH.
- Linux UNIX The user starting the IBM Business Monitor server must be profiled as an Oracle user profile.

### Oracle Instant Client

To use Oracle Instant Client, you must download and install the following libraries:

- Instant Client Package - Basic Instant Client Package
- SQL*Plus (useful for connection troubleshooting)

Add the installation directory to the server path and create a `TNSNAMES.ORA` file as described in the previous section. Add a TNS_ADMIN environment variable and specify the path to the directory containing the `TNSNAMES.ORA` file.

### 32-bit client requirement

An Oracle 32-bit client must be installed for IBM Cognos BI cube deployment. If Oracle is installed on a separate server, the 32-bit Oracle Instant Client is recommended. If Oracle is installed on the same server as IBM Cognos BI and 64-bit Oracle is installed, the 32-bit Oracle Instant Client must be installed as well.

If you are using 64-bit Oracle, complete the following steps to configure a path to the Oracle 32-bit libraries:

1. In the administrative console, click **Servers** > **Server types** > **WebSphere application servers** > ***server_name***. The Configuration panel is displayed.
2. Under **Server Infrastructure**, expand **Java and Process Management** and click **Process Definition**.
3. Under Additional Properties, click **Environment Entries**. Add the path to the Oracle Instant Client as described below:
   - Windows Add the path to the 32-bit Oracle Instant Client to the PATH environment variable using a ";" as a delimiter:
   - Linux UNIX Add the path to the 32-bit Oracle Instant Client to the following environment variable using a ":" as a delimiter.

     For Linux and Solaris: LD_LIBRARY_PATH

     For AIX: LIBPATH

## MONITOR database considerations for Microsoft SQL Server

There are specific recommendations for databases that are hosted on Microsoft SQL Server.

**Important:** When you are installing SQL Server, you must select mixed mode (Windows Authentication or SQL Server Authentication) as the authentication mode.

**Important:** To use SQL Server with IBM Business Monitor, you must configure SQL Server for XA transactions. SQL Server is not pre-configured for XA transactions. The XA support is delivered as part of the Microsoft JDBC driver distribution and contains a dynamic link library (sqljdbc_xa.dll) and an installation script (xa_install.sql). Because XA transactions are not enabled by default, you must change

the configuration in the Microsoft Windows Distributed Transaction Coordinator (MSDTC). For instructions to enable XA support for SQL Server, see "Understanding XA Transactions" in the Microsoft SQL Server online documentation.

When you are using the Profile Management Tool (in the WebSphere Customization Toolbox) or the manageprofiles command to create the SQL Server database, the database administrative user specified in the profile creation creates the database. The IBM Business Monitor runtime database user (@DB_USER@) that is specified during profile creation should already exist as an SQL Server login and database user. You can use the following command to create the database login and database user:

```
CREATE LOGIN @DB_USER@ WITH PASSWORD = '@DB_PASSWORD@', DEFAULT_DATABASE=@DB_NAME@
CREATE USER @DB_USER@ FOR LOGIN @DB_USER@
```

where DB_USER is the IBM Business Monitor runtime database user, DB_PASSWORD is the runtime database password, and DB_NAME is the IBM Business Monitor database name.

By default, the IBM Business Monitor runtime database user is granted db_owner privileges as part of the database creation. This enables the IBM Business Monitor server to automatically manage the monitor model database schema when models are deployed and removed. To secure the database, you can create the database manually and grant the runtime database user only the privileges required for runtime operations. See the topics "Installing the database manually" and "Securing the MONITOR database environment" in the related links.

The SQL Server JDBC drivers for JVM 1.6 provide JDBC support. IBM Business Monitor uses the Microsoft JDBC 2.0 driver `sqljdbc4.jar` file. By default, the Profile Management Tool points to the `sqljdbc4.jar` file supplied in **app_server_root\jdbcdrivers\SQLServer**. Alternatively, you can download another Microsoft `sqljdbc4.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command. For information about minimum required settings for SQL Server, see the related link.

## Globalization considerations

SQL Server manages the locale settings with the COLLATE option when creating the database. The create database statement for the MONITOR and COGNOSCS databases contains the following option:

```
COLLATE SQL_Latin1_General_CP1_CS_AS
```

To change the locale settings, change the collation parameter to a supported collation for the language you want. For example, to change the collation to French, you would use:

```
COLLATE French_100_CS_AS
```

SQL Server manages the default language based on the login user. To change the default language, in the `createDatabase.sql` file, add the DEFAULT_LANGUAGE option to the create login with a different default language. For example, to create the login with a default language of French, you would use:

```
 IF NOT EXISTS (SELECT * FROM syslogins WHERE NAME = '@DB_USER@')
CREATE LOGIN @DB_USER@ WITH PASSWORD = '@DB_PASSWORD@',
DEFAULT_DATABASE=@DB_NAME@, DEFAULT_LANGUAGE=French;
```

The DIM_TIME table contains a column for populating dashboard reports containing time dimensions with a translated month name. By default, the locale code for DEFAULT_LANGUAGE setting is used for populating the DIM_TIME table entries. To change the default language, change the DEFAULT_LANGUAGE for the database user before running the `createTables.sql` script.. There is also an SQL statement in `createTables.sql` that you can use to override the month name entries and define your own month names.

## Cognos database considerations for Microsoft SQL Server

IBM Cognos Business Intelligence uses the COGNOSCS (IBM Cognos BI content store) database for configuration and report specification information, and uses the MONITOR database for actual reporting data.

**Important:** The IBM Cognos BI database requires a case-insensitive collation while the IBM Business Monitor database requires a case-sensitive collation. If the default collation is changed for the IBM Cognos BI database, the collation must be case-insensitive.

### COGNOSCS database considerations for IBM Cognos BI

The IBM Cognos BI service creates tables in the IBM Cognos BI content store database the first time it is started. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

The COGNOSCS database must be used only for IBM Business Monitor data. You must not add data directly to the COGNOSCS database, or use the database with other databases to create reports against such data (combined or not with data created in IBM Business Monitor).

### MONITOR database considerations for IBM Cognos BI

If your MONITOR database is remote from the server or cluster that the IBM Cognos Business Intelligence service is deployed on, you must install a full Microsoft SQL Server database client on the IBM Cognos BI server to deploy cubes.

Microsoft offers a SQL Server Native Client that can be used in place of the full SQL Server client installation. This minimal installation includes all of the required native drivers. Along with the native client, you should also download and install the SQL Server command line utilities. Both items are available from the Microsoft SQL Server 2008 Feature Pack, August 2008 page.

IBM Cognos BI needs access to SQL Server client commands when publishing cube packages during model deployment. The SQL Server client must be in the server PATH.

## User registry considerations

The user registry stores information that is used to authenticate users using basic authentication. Your choice of user registry is an essential consideration when planning your environment. You must configure WebSphere Application Server to use the user registry in your environment.

The user registry stores information that is used to authenticate users requesting access to IBM Business Monitor. You can configure multiple user registry types under federated repositories. Most production deployments use a Lightweight Directory Access Protocol (LDAP) server. For small deployments that are contained on a single server, you can use a file-based user registry.

You can select any of the following for your user account repository:

- Federated Repositories
- Local operating system
- Standalone Lightweight Directory Access Protocol (LDAP) registry
- Standalone custom registry

**Note:** For fine-grained security, the supported user registries are federated repositories (file-based), federated repositories (LDAP), and standalone LDAP registry.

## Non-administrative user considerations

If you are installing IBM Business Monitor as a non-administrative or non-root user and you want to create a test profile during installation, you must have the DB2 server installed before you begin the installation. Remember the database details so that you can enter them during the installation.

The considerations described in this topic apply to any install scenario where you choose to install using the **Typical** install option. Profiles are created automatically when you install using the **Typical** option.

To install as a non-administrative user, you have the following choices: Linux Windows UNIX

- Before installing the product, install a DB2 server separately. For information about installing DB2 as a non-administrative or non-root user, see Linux UNIX Windows
  - Linux UNIX Non-root installation overview (Linux and UNIX)
  - Windows Required user accounts for installation of DB2 server products (Windows)
- Logon as an administrator and use the product installer to install the DB2 server alone. Grant special permission to the non-administrative user. Then logon as the non-administrative user and install the product using the installed DB2 server.

Alternatively, instead of creating a test profile, you can create a profile after installation . Use these steps:

1. Install the product without creating a profile. When you install as a non-administrative user, on the Install Packages page, you must clear the check box for DB2 Express. On Windows, if you have the option to install IBM Cognos Business Intelligence, you must clear that check box as well.
2. On the Features page, expand the servers and make sure that none of the test profiles are selected.
3. Use the Profile Management Tool to create a stand-alone profile, or to create the deployment manager and the custom profiles. If you do not have a database installed, use the **Advanced** path for all. Do not use the **Typical** path. Select the option to delay the execution of the database scripts during profile creation.
4. If the databases were not created in advance, have the database administrator create the databases and tables after profile creation or augmentation.
5. For a network deployment:
   a. Federate the custom profiles to the deployment manager.
   b. Using the administrative console, create the required deployment environment

## Topology considerations

In IBM Business Monitor, you can select from several different configuration paths to create your deployment environment.

A cross-cell environment is one in which IBM Business Monitor receives events from a server that is in a different cell from the IBM Business Monitor server. A cross-cell environment can involve either network deployment (ND) or single-server topology. In either case, you must perform several steps to enable communication between the common event infrastructure (CEI) server and the IBM Business Monitor server. For information on how to enable cross-cell communication, see "Configuring how to receive events." For an example of a cross-cell topology, see the "Monitoring events from an SAP enterprise information system (EIS) without mediation" scenario.

## Considerations for single-server topology

When you use the single-server topology, IBM Business Monitor and all required components are installed on the same physical server.

To install the IBM Business Monitor server and all required components on the same server, use the following high-level steps:

1. Complete the pre-installation steps found in Chapter 3, “Preparing to install,” on page 29.
2. Install IBM Business Monitor, following the steps in Chapter 4, “Installing the IBM Business Monitor software,” on page 35. When you install the product, you are given the option of creating a development profile, which provides a test environment but cannot be used in a production environment.
3. If you did not create a development profile, create a stand-alone profile using either the Profile Management Tool or the manageprofiles command, following the steps in Chapter 6, “Creating and augmenting profiles,” on page 69.

All required IBM Business Monitor components are installed and configured for you.

You can optionally check the status of the components and make updates using the configuration wizard in the administrative console.

## Considerations for network deployment topology using deployment environment patterns

Network deployment (ND) in IBM Business Monitor builds upon network deployment functions implemented in WebSphere Application Server Network Deployment. If you choose one of the available deployment environment patterns, use the deployment environment wizard to configure the clusters, servers, and components that you need.

If you are familiar with network deployment in WebSphere Application Server Network Deployment, the concepts are the same. For IBM Business Monitor, two patterns are available: the Single Cluster pattern and the Remote Messaging, Remote Support, and Web (four-cluster) pattern.

To install the IBM Business Monitor server and all required components using the single cluster or four-cluster deployment environment, use the following high-level steps:

1. Complete the pre-installation steps found in Chapter 3, “Preparing to install,” on page 29.
2. Install IBM Business Monitor, following the steps in Chapter 4, “Installing the IBM Business Monitor software,” on page 35. Do not create a development profile.
3. Create a deployment manager profile using either the Profile Management Tool or the manageprofiles command, following the steps in Chapter 6, “Creating and augmenting profiles,” on page 69.
4. Unless you created the MONITOR database as part of creating the profile, run the scripts to create the database, following the instructions in Chapter 5, “Creating the databases,” on page 49.
5. Start the deployment manager.
6. Create custom nodes that are federated into the deployment manager cell, following the steps in Chapter 6, “Creating and augmenting profiles,” on page 69.
7. Create the deployment environment, choosing either the Single Cluster pattern or the Remote Messaging, Remote Support, and Web (four-cluster) pattern. Follow the steps in “Creating the deployment environment using a pattern” on page 95.
8. Configure additional components such as Business Space and IBM Cognos BI, following the instructions in Chapter 10, “Configuring IBM Business Monitor components,” on page 127.

The clusters are created and all required IBM Business Monitor components are installed and configured for you.

You can optionally check the status of the components and make updates using the configuration wizard in the administrative console.

## Considerations for custom network deployment topology

Rather than use the deployment environment wizard to create a single-cluster or four-cluster topology for network deployment (ND), you can create any topology you choose using the configuration wizard or the wsadmin task.

To install the IBM Business Monitor server and all required components in a custom ND topology, use the following high-level steps:

1. Complete the pre-installation steps found in Chapter 3, "Preparing to install," on page 29.
2. Install IBM Business Monitor, following the steps in Chapter 4, "Installing the IBM Business Monitor software," on page 35. Do not create a development profile.
3. Create a deployment manager profile using either the Profile Management Tool or the manageprofiles command, following the steps in Chapter 6, "Creating and augmenting profiles," on page 69.
4. Unless you created the MONITOR database as part of creating the profile, run the scripts to create the database, following the instructions in Chapter 5, "Creating the databases," on page 49.
5. Start the deployment manager.
6. Create custom nodes that are federated into the deployment manager cell, following the steps in Chapter 6, "Creating and augmenting profiles," on page 69.
7. Use the administrative console to create the clusters, following the instructions in "Creating IBM Business Monitor clusters" on page 108.
8. Configure the required common event infrastructure (CEI) event services, following the instructions in "Configuring CEI event services" on page 110.
9. Use the configuration wizard or the wsadmin command to configure the environment, following the instructions in "Configuring the environment using the configuration wizard" on page 110 or "Configuring the environment using wsadmin commands" on page 115. For the required shared components, however, you must follow the manual steps provided in "Configuring the environment manually" on page 117.
10. Configure additional components such as Business Space and IBM Cognos BI, following the instructions in Chapter 10, "Configuring IBM Business Monitor components," on page 127.

## Considerations for IBM Business Process Manager in a four-cluster topology environment

You can configure a Four cluster topology with IBM Business Process manager to create a combined IBM® Business Process Manager and IBM Business Monitor deployment environment using the Remote Messaging, Remote Support, and Web (four-cluster) pattern. Because one IBM Business Monitor deployment environment can monitor all applications in the cell, you should only create one IBM Business Monitor deployment environment in a given cell. The four-cluster topology combines IBM Business Monitor and IBM Business Process Manager messaging engine clusters into a single cluster.

The following is the procedure to configure a four-cluster topology with IBM Business Process manager to create a combined IBM Business Process Manager and IBM Business Monitor deployment environment:

1. Complete the pre-installation steps found in the section Preparing to install.
2. Install IBM BPM product. Do not create a development profile.
3. Install IBM Monitor on the BPM WAS environment.
4. Create a deployment manager profile using either the Profile Management Tool or the **manageprofiles** command, following the steps in the section Creating and augmenting profiles.
5. Augment it to MONITOR deployment manager
6. Create CUSTOM profile of BPM which will be federated later
7. Augment it to MONITOR CUSTOM profile.

8. Start the deployment manager profile
9. Run the **AddNode** command to create custom profiles that are federated to deployment manager profile.
10. Configure the deployment environment step by step choosing the four-cluster pattern. Follow the steps in Creating the deployment environment using a pattern.

The clusters are created and all required IBM Business Monitor and IBM BPM components are installed and configured for you.

You can optionally check the status of the components and make updates using the configuration wizard in the administrative console.

**Related concepts**:

"Four-cluster topology" on page 7
You can install IBM Business Monitor into many topologies. You can use the four-cluster topology to set up a high performance environment.

# Chapter 3. Preparing to install

Before installing IBM Business Monitor, ensure that you have the required hardware and software prerequisites. Some operating platforms also require special preparation before you can install.

## Hardware and software requirements

IBM Business Monitor runs on AIX®, Windows, Linux, Linux on zSeries, Solaris, and z/OS operating systems.

For the most current software and hardware requirements, see the System requirements for IBM Business Monitor.

These links include supported LDAP servers. Stand-alone LDAP registries are also supported by IBM Business Monitor. All of the following current realm definitions are available for your current user account repositories:

- Federated Repositories
- Local operating system
- Standalone LDAP registry
- Standalone custom registry

## Preparing operating systems for product installation

Before you can install IBM Business Monitor, you must prepare your operating system. The configuration depends on the type of operating system you are using.

Before preparing the installation environment, complete the following tasks:

- Disable the firewall if you have a firewall running on the system where you plan to install IBM Business Monitor.
- Ensure that your user login provides access to your DB2 or Oracle database commands.
- Complete additional tasks specific to your operating system.

## Preparing AIX systems for installation

Before you can install IBM Business Monitor, you must prepare your AIX operating system.

Because WebSphere Application Server is a prerequisite of IBM Business Monitor, you must complete the required preparation steps in the Preparing the operating system for product installation topic in the WebSphere Application Server information center.

Because certain steps are specific to a version of the operating system, all steps might not apply to your environment. If no qualifier is provided for a particular step, complete the step for all versions of the operating system.

Refer to the following technote for additional preparation information for configuring Installation Manager to run on 64-bit AIX systems: https://www-304.ibm.com/support/docview.wss?uid=swg21330190.

Complete the following steps on your AIX system before installing IBM Business Monitor:

1. Increase the maximum number of open files. The default setting is usually not enough. You can check your current maximum number of open files by using **ulimit -n**. The following example shows the

© Copyright IBM Corp. 2005, 2012

maximum number of open files being increased to 8800, which is large enough for most systems. The ulimit requirement is dynamically calculated at installation time and might need to be larger based on the options you select.

Before installing, run the following command:

**ulimit -n 8800**

Alternatively, you can use the following steps to edit the resource limits file:

a. Open `/etc/security/limits`.
b. Edit or add the **default** section and include this line:

**nofiles = 8800**

c. Save and close the file.
d. Log off from the operating system and log in again.

2. Set the **umask** value to 022 using the following command:

**umask 022**

3. Ensure that you have Mozilla Firefox installed at version 3.5.x.x or higher.
4. Before starting the data movement service, increase the number of processes configured in the AIX operating system to avoid a connection reset error. You can increase the number of processing using a command, or using the AIX interface.
   - Run the command:

     ```
     chdev  -l sys0 -a maxuproc='256'
     ```

   - In the AIX interface, enter **smitty**, then select **System Environments > Change / Show Characteristics of Operating System > Number of processes allowed per user(Num.)**.
5. Complete the steps to Tune AIX systems.
6. Ensure all servers involved are set to the same time. Use the same network time protocol for all servers on all cluster nodes, including application, support, and database clusters. A time mismatch will cause erratic behavior, including duplicate system tasks.

## Preparing Linux systems for installation

Before you can install IBM Business Monitor, you must prepare your Linux operating system.

Because WebSphere Application Server is a prerequisite of IBM Business Monitor, you must complete all the required preparation steps in the Preparing the operating system for product installation topic in the WebSphere Application Server information center.

Ensure that you have Mozilla Firefox installed at version 3.5.x.x or higher.

Because certain steps are specific to a version of the operating system, all steps might not apply to your environment. If no qualifier is provided for a particular step, complete the step for all versions of the operating system. To install Installation Manager on Red Hat Enterprise Linux 6.0 (64-bit), see Unable to install Installation Manager on RHEL 6.0 (64-bit).

**Note:** Cognos bundles an alternate version of the libfreebl3.so library for Red Hat Enterprise Linux 6.0 (64-bit). Ensure that you preload this system library that is required for other utilities.

Complete the following steps on your Linux system before installing IBM Business Monitor:

1. If you are planning to install DB2 Express as part of the installation process, ensure that you have administrative (root) privileges. As a root user, you must also ensure that all kernel requirements are met before the DB2 Express installation begins. You can locate the current values by parsing the output of the **ipcs -l** command. To change the values, add the following lines, in the following order, to the `/etc/sysctl.conf` file:

```
kernel.shmmni=4096
kernel.shmmax=4294967296
kernel.shmall=8388608
#kernel.sem=<SEMMS><SEMMNS><SEMOPM><SEMMNI>
kernel.sem=250 256000 32 4096
kernel.msgmni=16384
kernel.msgmax=65536
kernel.msgmnb=65536
```

Reboot the system

2. Increase the allowable stack size, number of open files, and number of processes by adding the following lines to the end of the `/etc/security/limits.conf` file:

```
# - stack - max stack size (KB)
* soft stack 32768
* hard stack 32768
# - nofile - max number of open files
* soft nofile 65536
* hard nofile 65536
# - nproc - max number of processes
* soft nproc 16384
* hard nproc 16384
```

Save and close the file, and log off and log in again. You can check the current maximum number of open files by using **ulimit -n**. The **`ulimit`** requirement is dynamically calculated at installation time and might need to be larger based on the options you select. For more information about this setting, run **man limits.conf** or see the topic Preparing the operating system for product installation in the WebSphere Application Server information center.

3. Install the following packages for your operating system:

| Option | Description |
|---|---|
| **Red Hat Enterprise Linux 4** | compat-libstdc++-33-3.2.3-47.3<br>compat-db-4.1.25-9<br>xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2<br>rpm-build-4.3.3-7.nonptl<br>compat-libstdc++-296-2.96-132.7.2 |
| **Red Hat Enterprise Linux 5** | compat-libstdc++-33-3.2.3-61<br>compat-db-4.2.52-5.1<br>libXp-1.0.0-8<br>rpm-build-4.4.2-37.el5<br>**64-bit kernel only:** compat-libstdc++-296-2.96-138 |
| **Red Hat Enterprise Linux 6** | ksh-version.rpm Korn shell<br>See the detailed instructions and list of packages in Unable to install Installation Manager on RHEL 6.0 (64-bit) |
| **SUSE Linux Enterprise Server 9.0** | XFree86-libs-32bit-9<br>glibc-32bit-9<br>glib-32bit-9<br>gtk-32bit-9 |

You can also install a later release of any of these packages if there are new packages as errata. If you have additional packages that are specific to your hardware, install them.

You can use single-line commands to install dependencies (all required packages). The following commands are examples using the default package managers on supported Linux distributions.

- **Red Hat Enterprise Linux 5 (32-bit):**

  ```
  yum install compat-libstdc++-33 compat-db libXp rpm-build  RHEL 5.x
  ```

- **Red Hat Enterprise Linux 5 (64-bit):**

  ```
  yum install compat-libstdc++-33 compat-db libXp rpm-build compat-libstdc++-296
  ```

- **SUSE Linux:**

  ```
  zypper install XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9
  ```

4. Set the **umask** value to 022 using the following command:

   **umask 022**

5. On Red Hat Enterprise Linux 5 systems, disable SELinux, or set it to a permissive mode.
6. Restart the computer.
7. Complete the steps to Tune Linux systems.
8. Ensure all servers involved are set to the same time. Use the same network time protocol for all servers on all cluster nodes, including application, support, and database clusters. A time mismatch will cause erratic behavior, including duplicate system tasks.

## Preparing Solaris systems for installation

Before you can install IBM Business Monitor, you must prepare your Solaris operating system.

Because WebSphere Application Server is a prerequisite of IBM Business Monitor, you must complete the required preparation steps in the Preparing the operating system for product installation topic in the WebSphere Application Server information center.

The HotSpot Java JVM was developed by Sun Microsystems for the Solaris operating system. The Java heap structure and management for the HotSpot JVM is different from those of other JVMs. In your environment, you might need to tune the heap management of the JVM to avoid any **java.lang.OutOfMemoryError: PermGen** errors during profile creation or server runtime. You might need to update the value for the **MaxPermSize** JVM parameter.

Because certain steps are specific to a version of the operating system, all steps might not apply to your environment. If no qualifier is provided for a particular step, complete the step for all versions of the operating system.

Complete the following steps on your Solaris systems before installing IBM Business Monitor:

1. Increase the maximum number of open files. The default setting is usually not enough. You can check your current maximum number of open files by using **ulimit -n**. The following example shows the maximum number of open files being increased to 8800, which is large enough for most systems. The ulimit requirement is dynamically calculated at installation time and might need to be larger based on the options you select.

   Before installing, run the following command:

   **ulimit -Hn 8800**

   Alternatively, you can use the following steps to edit the resource limits file:

   a. Open /etc/system
   b. Add the following line to the end of the file:

      **set rlim_fd_max=8800**

   c. Save and close the file.
   d. Log off from the operating system and log in again.

2. Set the umask value to 022 using the following command:

   **umask 022**

3. Complete the steps to Tune Solaris systems.

4. Ensure all servers involved are set to the same time. Use the same network time protocol for all servers on all cluster nodes, including application, support, and database clusters. A time mismatch will cause erratic behavior, including duplicate system tasks.

Before creating or augmenting IBM Business Monitor profiles on your Solaris system, change the **MaxPermSize** JVM parameter, following the steps in Eliminating profile creation OutOfMemoryErrors on Solaris

## Preparing Windows systems for installation

Before you can install IBM Business Monitor, you must prepare your Windows operating system.

Because WebSphere Application Server is a prerequisite product for IBM Business Monitor, you must complete all of the preparation tasks for WebSphere Application Server before installing IBM Business Monitor.

Complete the following steps on your Windows system before installing IBM Business Monitor:

1. Complete the steps in the Preparing Windows systems for installation topic in the WebSphere Application Server information center.
2. Complete the steps to Tune Windows systems.

# Chapter 4. Installing the IBM Business Monitor software

You can install IBM Business Monitor interactively or silently. You can use IBM Business Monitor with other software in your monitoring environment, including WebSphere Portal or Process Server.

When you install IBM Business Monitor interactively, you must use the Installation Manager, whether you are installing all IBM Business Monitor components on a single server or installing the components to clusters in a network deployment environment.

Alternatively, you can set up a response file in advance and install IBM Business Monitor silently from a command line without interacting with the IBM Business Monitor installation program.

## Installing from the product launchpad

The IBM Business Monitor product launchpad program provides you with a single location to view release information for IBM Business Monitor, install WebSphere Application Server if required, and start the installation process.

Complete the preinstallation tasks described in Chapter 3, “Preparing to install,” on page 29, if you have not done so already.

For the default installation locations, see the related reference.

Windows To install or run IBM Business Monitor on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click `launchpad.exe` and select **Run as administrator**.

Use the product launchpad program to start the installation of IBM Business Monitor in the following cases:

- Installing from the product DVDs
- Installing from an electronic installation image on your local file system
- Installing from an electronic installation image on a shared drive

To start the launchpad program and install WebSphere Application Server if you have not already done so, complete the following steps. You can run only one launchpad at a time.

1. Insert the first IBM Business Monitor DVD into your DVD drive.

   Linux UNIX Ensure that you have mounted the DVD drive.
2. If auto-run is enabled on your system, the IBM Business Monitor launchpad program automatically opens. If auto-run is not enabled on your system:
   - Run **launchpad.sh** located in the root directory of the DVD.
   - Run **launchpad.exe**, or **launchpad64.exe** for a 64-bit system, located in the root directory of the DVD.
3. Optional: If you see a message that prompts you to update the launchpad, click **Update** to receive the latest updates. The updates are installed and your launchpad is restarted automatically.

   If you do not have access to the Internet and want updates to the launchpad to be installed from a local directory, you can use a properties file to tell the Installation Manager where to find the updates. Create the following file:

   - Linux UNIX `/home/user/bpm_updates.properties`
   - Windows `C:\HOMEPATH\bpm_updates.properties`

© Copyright IBM Corp. 2005, 2012

On Windows 7, Windows Vista, or Windows Server 2008, the HOMEPATH environment variable points to `C:\Users\user_name\`

For more information about Installation Manager updates, see Installation Manager updates.

**Note:** Ensure that you have read/write access to the folders specified in the `bpm_updates.properties` file.

The file uses a launchpad prefix, followed by a dot. The part of the name after the prefix and the dot can be anything you want, which enables you to point to multiple locations for launchpad upgrades. The locations can be either local directories or URLs. For example:

```
launchpad.1=http://test/launchpad
launchpad.2=C:\launchpad_updates
```

4. Optional: Click **Help System installation** to install the product Help System and documentation on your computer. The Help System is an Eclipse framework for displaying the documentation.
5. If you are in the Administrator group on Windows, or if you are a root user on a Linux or UNIX system, ensure that **Install as administrative user** is selected. Clear this check box only if you are not an administrative user, or if you want to install to your own user name without giving privileges to other users.
6. **If you do not yet have WebSphere Application Server installed**, click the **Install** button to start the installation of IBM Business Monitor.

   **Important:** If you are on a 64-bit system, you might receive the following message:

   ```
   Your operating system failed the launchpad prerequisites check. The following 32-bit GTK Library
   for running IBM Installation Manager is not available in underlying OS:
   list_of_missing_files. Please install the 32-bit GTK Library and restart your installation.
   ```

   If you see this message, your server does not have the 32-bit version of the GTK library installed, or the library is an incorrect version. Update your server with the correct version of the 32-bit GTK library, using the DVD or official web site of your operating system, before you continue the installation.
   The Installation Manager is started and configured for you. Go to "Installing IBM Business Monitor interactively" on page 37 for the remainder of the installation instructions.
7. **To install IBM Business Monitor on an existing installation of WebSphere Application Server**, click **Installation on existing WebSphere Application Server**.
   a. If you are in the Administrator group on Windows, or if you are a root user on a Linux or UNIX system, ensure that **Install as administrative user** is selected. Clear this check box only if you are not an administrative user, or if you want to install to your own user name without giving privileges to other users.
   b. Click **Import or Update**.
      - If the Open file window displays, click **Run**. The Installation Manager opens.
      - Click **Import** to import WebSphere Application Server into Installation Manager. You must import WebSphere Application Server if it has never previously been imported or if it has been updated with the Update Installer after it was last imported.
      - Click **Browse** and select the directory where WebSphere Application Server was installed, for example, **app_server_root**.
      - Click **Next**, and then click **Import**.
      - Click **Finish**.
      - From the Installation Manager window, click **Update**.
      - Select the package group **IBM WebSphere Application Server - ND**.

        **Tip:** On the Update Packages page, select **Show All** to display available updates.
      - Click **Next** and follow the instructions on each page, accepting the defaults.
      - Close the Installation Manager and return to the launchpad application.

c. Click **Install** to start the installation of IBM Business Monitor. If the Open file window displays, click **Run**.

   **Important:** If you are on a 64-bit system, you might receive the following message:

   ```
   Your operating system failed the launchpad prerequisites check. The following 32-bit GTK Library
   for running IBM Installation Manager is not available in underlying OS:
   list_of_missing_files. Please install the 32-bit GTK Library and restart your installation.
   ```

   If you see this message, your server does not have the 32-bit version of the GTK library installed, or the library is an incorrect version. Update your server with the correct version of the 32-bit GTK library, using the DVD or official web site of your operating system, before you continue the installation.

d. Click **Install IBM Business Monitor**. The Installation Manager is started and configured for you. Go to "Installing IBM Business Monitor interactively" for the remainder of the installation instructions.

If your operating system supports it, you can click **Help System Installation** on the launchpad to install the information center.

## Installing IBM Business Monitor interactively

You can install IBM Business Monitor interactively using the Installation Manager, whether you are installing all the components on a single server or installing the components to clusters in a network deployment environment.

Launch the Installation Manager from the product launchpad. For the default installation locations, see the related reference link.

To install IBM Business Monitor, complete the following steps:

1. From the Installation Manager Start page, click **Install Packages** and click **Next** to continue. The following packages are selected for you:

   **IBM Cognos Business Intelligence**
   Clear this check box if you are using Microsoft Windows and you are not an administrative user.

   **WebSphere Application Server - ND**
   Clear this check box if the package is already installed.

   **DB2 Express®**
   Clear this check box if you already have a database that you intend to use or if you are not an administrative user.

   **IBM Business Monitor**

   If you receive the following warning message during the prerequisite checking, use the platform-specific steps below to increase the **ulimit** number.

   ```
   Current system has detected a lower level of ulimit than the recommended value of recommended_value.
   Please increase the ulimit number to minimum value of recommended_value and re-start the installation.

   Shutdown your installer. If you are a root user open a command prompt and issue ulimit -n
   recommended_value and then restart the installer. If you are a non-root user, work with your
   system administrator to increase your ulimit -n recommended_value and then restart the
   installer.
   ```

   The required value is calculated based on the version of WebSphere Application Server and the configuration that you are installing.

   a. Set the maximum number of open files using the following steps: Linux

      1) Open `/etc/security/limits.conf`.

2) Locate the **nofile** parameter and increase the value. If a line containing the **nofile** parameter does not exist, add the following lines to the file:

   * **hard nofile** *recommended_value*

   * **soft nofile** *recommended_value*

3) Save and close the file.

4) Log off and log in again.

b. Restart the computer.

c. Restart the installer.

2. On the Licenses page, read the license agreement for the selected package.

   If you selected more than one package to install, there might be a license agreement for each package. On the left side of the **License** page, click each package version to display its license agreement. The package versions that you selected to install (for example, the base package and an update) are listed under the package name.

   a. If you agree to the terms of all of the license agreements, click **I accept the terms of the license agreements**.

   b. Click **Next**.

3. If IBM Business Monitor is the first package installed using Installation Manager, enter the path for the *shared resources directory* in the **Shared Resources Directory** field on the Location page, or accept the default path. The shared resources directory contains resources that can be shared by one or more package groups.

   **Important:**

   a. You can specify the shared resources directory only the first time that you install a package. Use your largest disk for this to ensure adequate space for the shared resources of future packages. You cannot change the directory location unless you uninstall all packages.

   b. Ensure that your installation path does not contain parentheses.

   c. Linux UNIX Ensure that your installation path does not contain spaces.

   Click **Next**.

4. On the next Location page, create a *package group* to install the IBM Business Monitor package into. To create a new package group use the following steps:

   a. Select **Create a new package group**.

   b. Type the path for the installation directory for the package group. Ensure that your installation path does not contain parentheses. Linux UNIX Do not include any spaces in the directory path. The name for the package group is created automatically.

   c. Click **Next**.

      The Install Packages wizard displays a message if it detects any running processes (such as the WebSphere Application Server server). If you see the message, click **Cancel**, shut down the running processes, and begin the installation again.

5. On the Features page, select the package features to install.

   a. Optional: To see the dependency relationships between features, select the **Show Dependencies** check box.

   b. Optional: Click a feature to view its brief description under **Details**.

   c. Select or clear features in the package. Installation Manager automatically enforces any dependencies with other features and display updated download size and disk space requirements for the installation.

      - If you do not select any features, Business Space and the IBM Business Monitor license files are installed.

- If you expand **Business Monitor Server** and select one or more stand-alone development profiles, the profiles are created for you during installation. To create Process Server or WebSphere Enterprise Service Bus development profiles, you must have those packages already installed.

  A stand-alone development profile is a default development profile that provides a IBM Business Monitor test environment. The Process Server development profile also comes with Business Process Rules Manager enabled. To create a stand-alone development profile, you must supply the administration security credentials (user name and password) for the server that you are creating.

  A stand-alone development profile cannot be used in a production environment. If you choose not to install a default stand-alone development profile, you can install one later by launching the Installation Manager and clicking **Modify** on the first page.

  If you are installing **Business Monitor Server** 8.0, and you have profiles that were previously created, those profiles are automatically preserved. You do not need to re-create them.

d. Required: Select the WebSphere Application Server feature **EJBDeploy tool for pre-EJB 3.0 modules**. This feature is selected by default. If it is not selected, some **Business Monitor Server** 8.0 components may not work correctly.

e. When you are finished selecting features, click **Next**.

6. If you selected a stand-alone development profile, on the Profiles page, enter the credentials for your profile. The default user name is `admin` and the default password is `admin`.

7. On the Common Configurations page, if you already have a database, enter the credentials for the database. If you selected DB2 Express, enter a user name and password for DB2. The default administrative user name is `bpmadmin`. Choose a password that complies with the password policy of your system (for example, Windows 2008).

   **Restriction:** User names must not contain National Language Strings (NLS).
   Click **Next**.

8. On the Summary page, review your choices before installing the IBM Business Monitor package.
   - If you want to change the choices that you made on previous pages, click **Back** and make your changes.
   - If you are satisfied with your installation choices, click **Install** to install the package

   A progress indicator shows the percentage of the installation completed.

9. When the installation process is complete, a message confirms the success of the process. If you chose to create a stand-alone development profile during installation and it failed or did not fully succeed, you see an error message informing you of the failure and giving you the location of the profile creation error log at app_server_root/`logs/manageprofiles/`*`profilename`*`_create.log`. You must resolve the profile creation problem and create a profile using the Profile Management Tool or the **`manageprofiles`** command.

   a. Optional: Click **View log file** to open the installation log file for the current session in a new window. You must close the Installation Log window to continue.

   b. Under **Which program do you want to start?**, select whether you want the Profile Management Tool to start when you exit. If you have already created a stand-alone development profile, you can select **None**. For production, you must define a stand-alone server profile or a deployment manager using the Profile Management Tool or the **`manageprofiles`** command. See the information about *Creating and Augmenting profiles*.

   c. Click **Finish** to close the Installation Manager.

For production, you must create a stand-alone server profile or a deployment manager using the Profile Management Tool or the **`manageprofiles`** command.

**Restriction:** If you created a stand-alone development profile during installation, remember that it does not work in a production environment. It is intended to help you gain familiarity with IBM Business Monitor without having to create a working production profile. You can start the profile from its First steps console.

- Open a command window. Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
- Go to **Start** > **All Programs** > **IBM** > **Business Monitor 8.0** > **Profiles** > *profile_name* > **First Steps**.
- Go to **profile_root\firststeps.wbm** and run the **firststeps.bat** command.

  **Important:** To install or run First Steps on Microsoft Windows 7, Microsoft Windows Vista, or Microsoft Windows Server 2008, you must elevate your Microsoft Windows user account privileges by right-clicking **firststeps.bat** and selecting **Run as administrator**. This is required for both administrative and nonadministrative users.

## Installing IBM Business Monitor silently

You can install the IBM Business Monitor product package in *silent* installation mode. When you install in silent mode, the user interface is not available.

**Important:** Only one IBM Installation Manager is required to install multiple instances of IBM Business Monitor.

## Installing IBM Business Monitor silently using the command line

You can install IBM Business Monitor using the command line.

Before you install IBM Business Monitor, review the system requirements for the product.

Operating system and software prerequisite levels are particularly important. Although the installation process automatically checks for prerequisite operating system patches, review the system requirements if you have not already done so. The system requirements link lists all supported operating systems and the operating system fixes and patches that you must install to have a compliant operating system. It also lists the required levels of all prerequisite software.

If you are planning to install IBM Business Monitor using DB2 Express with Red Hat Enterprise Linux 6, ensure that the user has administrative privileges (root user). As a root user, you must also ensure that all kernel requirements are met before the DB2 Express installation begins. You can locate the current values by parsing the output of the **ipcs -l** command.

If you do not have the prerequisite base products necessary for IBM Business Monitor installation, you must install them as part of the silent installation. The required base products are:

- Installation Manager
- WebSphere Application Server Network Deployment, including the ejbdeploy and thinclient features

The silent installation performs the following tasks:

- Installs Installation Manager if it is not already installed or updates it to the appropriate level if it is installed.
- Installs the required base products and IBM Business Monitor.

To silently install IBM Business Monitor, complete the following steps:

1. Run the following command to generate encrypted passwords using IBM Installation Manager to securely connect to DB2 and the WebSphere administrative console.

**Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.

Windows

```
IM_location\eclipse\tools\imutilsc -silent -nosplash encryptString password_to_encrypt
```

Linux

```
IM_location/eclipse/tools/imutilsc -silent -nosplash encryptString password_to_encrypt
```

2. Read and accept the license terms before installing. Adding **-acceptLicense** to the command line means that you accept all licenses.
3. Run the following command:

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.

   Windows

```
extract_directory\IM\tools\imcl install list_of_product_IDs -acceptLicense
-installationDirectory location -repositories repository
-properties key=value,key=value -showVerboseProgress -log logName.log
```

   UNIX Linux

```
extract_directory/IM/tools/imcl install list_of_product_IDs -acceptLicense
-installationDirectory location -repositories repository
-properties key=value,key=value -showVerboseProgress -log logName.log
```

   where:

   - *list_of_product_IDs* is a list of the IDs for the products you want to install, separated by spaces.

*Table 1. Product IDs*

| Product | Product ID | Feature | Description |
|---|---|---|---|
| IBM Business Monitor | com.ibm.websphere.MON.V80 | core.feature | Required. IBM Business Monitor core runtime content. |
| | | wbm.server.feature | Required. IBM Business Monitor server runtime content. |
| | | wbm.profile.feature | Stand-alone development IBM Business Monitor profile (qmwas). |
| | | wbm.wps.profile.feature | Stand-alone development IBM Business Monitor on Process Server profile (qmbpmaps). |
| | | wbm.esb.profile.feature | Stand-alone development IBM Business Monitor on WebSphere ESB profile (qmesb). |

*Table 1. Product IDs (continued)*

| Product | Product ID | Feature | Description |
|---|---|---|---|
| WebSphere Application Server Network Deployment | com.ibm.websphere.ND.v80 | core.feature | Required. WebSphere Application Server core content. |
| | | ejbdeploy | Required. Pre-Enterprise JavaBeans (EJB) 3.0 modules. |
| | | thinclient | Required. Stand-alone thin clients and resource adapters. |
| | | embeddablecontainer | Embeddable EJB container. |
| | | samples | Sample applications feature. |
| | | com.ibm.sdk.6_32bit | 32-bit software development kit (SDK). You must specify either this feature or com.ibm.sdk.6_64bit. |
| | | com.ibm.sdk.6_64bit | 64-bit SDK This feature can only be selected on a 64-bit system. You must specify either this feature or com.ibm.sdk.6_32bit. |
| Installation Manager | com.ibm.cic.agent | agent_core | Installation Manager core content. |
| | | agent_jre | Installation Manager Java Runtime Environment (JRE). |
| DB2 Express for Linux 32-bit | com.ibm.ws.DB2EXP97. linuxia32 | n/a | DB2 must match the operating system and bitness. |
| DB2 Express for Linux 64-bit | com.ibm.ws.DB2EXP97. linuxia64 | n/a | DB2 must match the operating system and bitness. |
| DB2 Express for Windows 32-bit | com.ibm.ws.DB2EXP97. winia32 | n/a | DB2 must match the operating system and bitness. |
| DB2 Express for Windows 64-bit | com.ibm.ws.DB2EXP97. winia64 | n/a | DB2 must match the operating system and bitness. |
| IBM Cognos Business Intelligence for Windows x86 (32-bit) | com.ibm.ws.cognos.v1011. winia32 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitness. |
| IBM Cognos BI for Windows x64 (64-bit) | com.ibm.ws.cognos.v1011. winia64 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for AIX PPC 32-bit | com.ibm.ws.cognos.v1011. aix32 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |

*Table 1. Product IDs (continued)*

| Product | Product ID | Feature | Description |
|---|---|---|---|
| IBM Cognos BI for AIX PPC 64-bit | com.ibm.ws.cognos.v1011.aix64 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for Linux x86 (32-bit) | com.ibm.ws.cognos.v1011.linuxia32 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for Linux x86-64 (64-bit) | com.ibm.ws.cognos.v1011.linuxia64 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for Solaris SPARC (32-bit) | com.ibm.ws.cognos.v1011.solaris32 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for Solaris SPARC (64-bit) | com.ibm.ws.cognos.v1011.solaris64 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |
| IBM Cognos BI for Linux on System z | com.ibm.ws.cognos.v1011.zlinux64 | n/a | IBM Cognos BI must match the operating system and the WebSphere Application Server bitnes |

- *location* is the path to the directory where you want to install the products.
- *repository* is the path to the repository where you have extracted the files, one of the following directories:

  ```
  extract_directory/repository/repos_32bit
  extract_directory/repository/repos_64bit
  ```

  For more than one repository, separate the repository locations with commas.
- *key=value* is a list of the keys and values you want to pass to the installation, separated by commas. Do not put spaces between the commas. Create encrypted passwords using the IBM Installation Manager.

*Table 2. Keys*

| Key | Description |
|---|---|
| user.select.64bit.image | If you are installing on a 64-bit operating system, add the following line exactly:<br>`user.select.64bit.image,,com.ibm.websphere.ND.v80=true`<br><br>The default value is false. |
| user.db2.admin.username | Windows only. User name with authority to access the DB2 database. The default value is bpmadmin. |
| user.db2.admin.password | Windows only. Password for the user name above. Choose a password that complies with the password policy of your system (for example, Windows 2008). |

*Table 2. Keys (continued)*

| Key | Description |
|---|---|
| user.bpm.admin.username | User name for the administrative console. The default value is admin. This property is needed only if you are creating a profile. |
| user.bpm.admin.password | Password for the user name above. The default value is admin. This property is needed only if you are creating a profile. |
| user.db2.port | Port for the DB2 database. The default value is 50000. |
| user.db2.instance.username | Linux only. DB2 instance user name. The default value is bpminst. |
| user.db2.instance.password | Linux only. Password for the user name above. |
| user.db2.fenced.username | Linux only. Fenced user name. The default value is bpmfenc. |
| user.db2.fenced.password | Linux only. Password for the user name above. |
| user.db2.das.username | Linux only. Administration server (DAS) user name. The default value is bpmadmin. |
| user.db2.das.password | Linux only. Password for the user name above. |

- *logName* is the name of the log file to record messages and results.

Running this command installs the product with the default features. If you want to install specific features or make other changes, see the reference link for the command-line arguments for imcl.

Installation Manager installs the list of products and writes a log file to the directory that you specified.

The following example installs IBM Business Monitor.

Windows

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80,core.feature,ejbdeploy,thinclient,
embeddablecontainer,samples,com.ibm.sdk.6_32bit com.ibm.ws.cognos.v1011.winia32
com.ibm.ws.DB2EXP97.winia32 -acceptLicense
-installationDirectory C:\IBM\MON80 -repositories D:\temp\MonServer\repository\WBM
-properties user.db2.admin.username=bpmadmin,user.db2.admin.password=Vvrs88V/a9BUdxwodz0nUg==
-showVerboseProgress -log silentinstall.log
```

Linux

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80,core.feature,ejbdeploy,thinclient,
embeddablecontainer,samples,com.ibm.sdk.6_32bit com.ibm.ws.cognos.v1011.linuxia32
com.ibm.ws.DB2EXP97.linuxia32 -acceptLicense
-installationDirectory /usr/IBM/MON80 -repositories usr/tmp/MonServer/repository/WBM
-properties user.db2.instance.username=bpmadmin,user.db2.instance.password=Vvrs88V/a9BUdxwodz0nUg==
-showVerboseProgress -log silentinstall.log
```

AIX

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80,core.feature,ejbdeploy,thinclient,
embeddablecontainer,samples,com.ibm.sdk.6_32bit com.ibm.ws.cognos.v1011.aix32 -acceptLicense
-installationDirectory /usr/IBM/MON80 -repositories usr/tmp/MonServer/repository/WBM
-showVerboseProgress -log silentinstall.log
```

Solaris

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80,core.feature,ejbdeploy,thinclient,
embeddablecontainer,samples,com.ibm.sdk.6_32bit com.ibm.ws.cognos.v1011.solaris32 -acceptLicense
-installationDirectory /usr/IBM/MON80 -repositories usr/tmp/MonServer/repository/WBM
-showVerboseProgress -log silentinstall.log
```

You must define a stand-alone server profile or a deployment manager in the Profile Management Tool or using the manageprofiles command. Only profiles created with the Profile Management Tool or manageprofiles command can be used in production.

## Installing IBM Business Monitor silently using a response file

You can install IBM Business Monitor by creating a response file and then running a command to use that response file to install the product.

Before you install IBM Business Monitor, review the system requirements for the product.

Operating system and software prerequisite levels are particularly important. Although the installation process automatically checks for prerequisite operating system patches, review the system requirements if you have not already done so. The system requirements link lists all supported operating systems and the operating system fixes and patches that you must install to have a compliant operating system. It also lists the required levels of all prerequisite software.

If you are planning to install IBM Business Monitor using DB2 Express with Red Hat Enterprise Linux 6, ensure that the user has administrative privileges (root user). As a root user, you must also ensure that all kernel requirements are met before the DB2 Express installation begins. You can locate the current values by parsing the output of the **ipcs -l** command.

If you do not have the prerequisite base products necessary for IBM Business Monitor installation, you must install them as part of the silent installation. The required base products are:

- Installation Manager
- WebSphere Application Server Network Deployment, including the ejbdeploy and thinclient features

The silent installation performs the following tasks:

- Installs Installation Manager if it is not already installed or updates it to the appropriate level if it is installed.
- Installs the required base products and IBM Business Monitor.

To silently install IBM Business Monitor, complete the following steps:

1. Run the following command to generate encrypted passwords using IBM Installation Manager to securely connect to DB2 and the WebSphere administrative console.

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.

   Windows

   ```
   IM_location\eclipse\tools\imutilsc -silent -nosplash encryptString password_to_encrypt
   ```

   Linux

   ```
   IM_location/eclipse/tools/imutilsc -silent -nosplash encryptString password_to_encrypt
   ```

2. Read and accept the license terms before installing. Adding **-acceptLicense** to the command line means that you accept all licenses.
3. Create the response file that will install the required base products and IBM Business Monitor. Copy the sample response file from the following directory to create your own response file:

   ```
   extract_directory/responsefiles/WBM/template_response.xml
   ```

4. Modify the parameters as directed in the text of the response file template to create your response file. You can also create a response file by recording your actions in Installation Manager. When you record a response file, the selections that you make in Installation Manager are stored in an XML file. When you run Installation Manager in silent mode, Installation Manager uses the data in the XML response file to perform the installation.

   **Important:** Verify that the repository locations at the top of the sample response file point to the correct location in your environment.
5. Run the following command:

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.

   Administrator or Root user: Windows

   ```
   extract_directory\IM\installc.exe -acceptLicense input
   extract_directory\responsefiles\BusMon\template_response.xml
   -log preferred_log_location\silent_install.log
   ```

   UNIX Linux

   ```
   extract_directory/IM/installc -acceptLicense input
   extract_directory/responsefiles/BusMon/template_response.xml
   -log preferred_log_location/silent_install.log
   ```

   Non-administrator or non-root user: Windows

   ```
   extract_directory\IM\userinstc.exe -acceptLicense input
   extract_directory\responsefiles\BusMon\template_response.xml
   -log preferred_log_location\silent_install.log
   ```

   UNIX Linux

   ```
   extract_directory/IM/userinstc -acceptLicense input
   extract_directory/responsefiles/BusMon/template_response.xml
   -log preferred_log_location/silent_install.log
   ```

Installation Manager installs any required prerequisites and IBM Business Monitor, and writes a log file to the directory you specified.

You must define a stand-alone server profile or a deployment manager in the Profile Management Tool or using the manageprofiles command. Only profiles created with the Profile Management Tool or manageprofiles command can be used in production.

## Installing the information center

The IBM Business Monitor information center is available on the Internet. You can also install it from the product launchpad if it is supported on your operating system.

- Install and start the information center from the product launchpad.
  1. From the launchpad, click **Help System installation**.
  2. Specify the location for the local information center.
  3. Click **Install and start the Help System**. If the Open file window displays, click **Run**.
- View the information center on the Internet. See the IBM Business Process Management Information Center

## Starting and stopping the local information center

After you have installed the IBM Business Monitor information center, you can view the information on your local system or to host it for access for other users in your network.

In this procedure, **doc_root** represents the directory where you chose to install the information center.

- To view the information center locally, complete the following steps:
  1. Change directories to the directory where you installed the information center.
  2. To start the information center, run the script that is appropriate for your operating system:
     - **help_start.sh**
     - **help_start.bat**

     Your default browser opens and displays the information center that was installed with the product.
  3. To stop the information center, close the browser and run the script that is appropriate for your operating system:
     - **help_end.sh**
     - **help_end.bat**
- To host the information center and view on other systems in your network, complete the following steps:
  1. Change directories to the directory where IBM Business Monitor is installed.
  2. To start the information center, run the script that is appropriate for your operating system:
     - **IC_start.sh**
     - **IC_start.bat**

     Users can open a browser, and navigate to the following URL to access the information center from another system:

     `http://host_name:8888/help/index.jsp`
  3. To stop the information center, close the browser and run the script that is appropriate for your operating system:
     - **IC_end.sh**
     - **IC_end.bat**

## Updating the local information center

Your locally installed version of the documentation can be updated as new documentation becomes available if you have an Internet connection. Other products might also have updated documentation that you can pull into your local information center.

To update the documentation, complete the following steps:

1. Click the **Update** icon ( ) in the help system toolbar. You see a list of any documentation sets that are already installed.
2. Click **Next** at the bottom of the installed documentation list. You see a list of documentation sets to install. These sets include product documentation in different languages and can also include documentation sets for different products.
3. Select the documentation that you want to install.

   **Tip:** You can select more than one set of documentation.

The documentation for the product or products you selected is installed in the help system on your computer.

# Chapter 5. Creating the databases

IBM Business Monitor requires two databases, one for the IBM Business Monitor configuration and one for the IBM Cognos Business Intelligence content store.

## MONITOR and COGNOSCS databases

By default, the database for IBM Business Monitor is named MONITOR and the database for the IBM Cognos BI content store is named COGNOSCS.

You can create the MONITOR and COGNOSCS databases as part of creating a stand-alone or deployment manager profile, you can use the database design tool (dbDesignGenerator), or you can manually create the databases by running the database script files before or after profile creation. In a network deployment environment, it is best to create the databases before starting the deployment manager and creating custom profiles.

**Important:** If you are using DB2 for z/OS, create the database using the database design tool (dbDesignGenerator) or manually create the database.

If you have an existing IBM Cognos BI server, you do not need to create a COGNOSCS database because the content store is already defined.

**Tip:** If the COGNOSCS database is remote from the IBM Cognos BI server, you must install a database client on the IBM Cognos BI server machine. See the details in the database-specific database consideration topics.

The MONITOR and COGNOSCS databases can be located on the same server as the IBM Business Monitor server or on a different server. For profile creation to create the databases automatically, your database server must be local to the machine where you run the Profile Management Tool or the **manageprofiles** command. Otherwise, use the database script files to create the databases. Also use the database script files to create the databases if you are using z/OS, or if the database server contains multiple versions of the database or multiple database instances.

## Database scripts

When you create a stand-alone or deployment manager profile, database scripts are generated that match the values entered during profile creation, ensuring that names are consistent between the IBM Business Monitor server and the IBM Business Monitor database.

You can also create the database scripts yourself using one of the following methods:

- Configure the values using the database design tool (DbDesignGenerator) that is installed with the IBM Business Monitor server. One advantage of using the database design tool is that you can design the MONITOR database, the IBM Cognos BI database, the Business Space database, and the databases for the messaging engines for IBM Business Monitor and the common event infrastructure (CEI) all at the same time. See “Creating or configuring database scripts using the database design tool” on page 50 for instructions.
- Configure the values manually. See “Configuring MONITOR database scripts manually” on page 51 for instructions.

After the database scripts are generated or customized, run the scripts using the procedures described in “Installing the MONITOR database manually” on page 55.

© Copyright IBM Corp. 2005, 2012

### Messaging engine tables

The messaging engines for the IBM Business Monitor service integration bus and the common event infrastructure (CEI) bus require database tables. Except on z/OS, these tables can be created automatically by WebSphere Application Server if the IBM Business Monitor database user has sufficient privileges and the option to create tables automatically is set in the service integration bus message store options. This option is set to true by default unless you are using DB2 for z/OS.

The database scripts for the messaging engine tables can also be generated using one of the following options:

- Create the script using the database design tool (DbDesignGenerator). See "Creating or configuring database scripts using the database design tool" for instructions.
- Create the tables manually. See "Creating messaging engine tables manually" on page 57 for instructions.

### Business Space tables

If you are using Business Space, you must also configure the Business Space tables, using either the scripts that were generated during stand-alone profile creation or the database design tool. For more information, see Configuring Business Space database tables in the Business Space information center.

### Database security

When the databases are created, the runtime database user is granted privileges to administer database objects by default, which simplifies the creation of the databases and enables the IBM Business Monitor server to automatically manage the monitor model database schema when models are deployed and removed. If you must secure the databases, see Securing the MONITOR database environment and Configuring IBM Cognos BI security.

## Creating or configuring database scripts using the database design tool

The database design tool (DbDesignGenerator) installed with the IBM Business Monitor server can be used to generate database scripts that can be executed before or after IBM Business Monitor profile creation.

One advantage of using the database design tool is that you can design the databases for IBM Business Monitor, IBM Cognos BI, Business Space, and the messaging engine all at the same time. Database scripts are generated for each component, and a dbdesign file is generated that can later be passed into the deployment environment wizard, to automatically configure the data sources when creating a complex IBM Business Monitor topology.

**Important:** Make sure you use the database design tool when you are creating databases for DB2 for z/OS.

If you choose the **Advanced** path through the Profile Management Tool, you can choose **Configure the database using a design file** and select a design file that you have already created.

For more information about the database design tool, see the related links.

To edit the database script files using the database design tool, complete the following steps:

1. Change directory to the **app_server_root/util/dbUtils** directory.
2. Run the command to start the utility.
   - DbDesignGenerator.bat

- DbDesignGenerator.sh.

3. From the main menu, select option **(1) Create a database design for Standalone profile or Deployment Environment**.
4. At the **Please pick one of the following db designs that are supported** prompt, select either option **(1)monitor.nd.topology** or option **(2)monitor.standalone**. The monitor.nd.topology option provides more flexibility for distributing the database components across multiple databases.
5. At the **Please pick one of the following [database component(s)]** prompt, select option **(1)[Monitor] MONITOR : [master] [status = not complete]**.
6. At the **Edit this db component?** prompt, enter **y**.
7. At the **Please pick one of the following DB types that are supported** prompt, select the number of your database platform.
8. Respond to the series of prompts or press Enter to accept the defaults where applicable. You are asked to enter your database name, schema name, user name and password, and table space location directory prefix.
9. At the **To skip data source properties, enter 's'; or enter anything else to continue** prompt, enter **c** (or any character except **s**) to continue entering information.
10. Respond to the series of prompts or press Enter to accept the defaults where applicable. You are asked to enter the properties for your data source.
11. Verify that the IBM Business Monitor database component is complete before configuring the other components. The IBM Cognos BI database is shown as not complete and requires a database user and password. You can accept the defaults for the other settings.
12. When you see the **Please pick one of the following [database component(s)]** prompt again, you have finished entering properties if all the lines display **[status = complete]**, for example **(1)[Monitor] MONITOR : [master] [status = complete]**. Enter **5 [save and exit]** and press Enter to save the database design.

    The **[Cognos] COGNOSCS** database component requires additional configuration after completing the MONITOR configuration. The COGNOSCS status is **[status = not complete]** until this component is fully configured.
13. At the **Please enter the output directory** prompt, press Enter to accept the default (**app_server_root/util/dbUtils**) or enter the location to write the database design files.
14. At the **Please enter the output filename** prompt, press Enter to accept the default (**monitor.standalone.dbdesign**) or enter the name for the file.
15. At the **Generate db script?** prompt, enter **y** and keep pressing Enter to accept the default locations. Subdirectories are created for the MONITOR and COGNOSCS database scripts, messaging engine datastore script, and Business Space database scripts.

## Configuring MONITOR database scripts manually

The database scripts required for creating the MONITOR database are shipped on the installation media and are copied to the application server during IBM Business Monitor server installation. These database scripts can be customized manually so that you can create the databases before server installation or profile creation.

To edit the database script files manually, complete the following steps:

1. Using a text editor, open the database script files for your database software.

   The scripts create the databases and required tables for IBM Business Monitor.

   - **For DB2 for z/OS**:
     - **createDatabase_Monitor.sql**
     - **createTablespace_Monitor.sql**
     - **createTable_Monitor.sql**
   - **For all other databases:**

– **createDatabase.sql**
– **createTables.sql**

By default, the files are located in the following directories:

(distributed only) *DVD_root*/scripts/database/Monitor/*platform*

app_server_root/dbscripts/Monitor

app_server_root/profiles/*profile_name*/dbscripts/Monitor (stand-alone)

app_server_root/profiles/*profile_name*/dbscripts.wbm (deployment manager)

where

*DVD_root* is the directory where you extracted the DVD or downloadable image

*platform* is the operating system of the database (for example DB2, Oracle, or SQL Server)

*app_server_root* is the directory where IBM Business Monitor is installed

2. Edit the following variables in the database script files for your database software:
   - **For DB2**, edit the following variables:

     **@DB_NAME@**
     Represents the name of the IBM Business Monitor database (for example, MONITOR).

     **@SCHEMA@**
     Represents the name of the IBM Business Monitor schema (for example, MONITOR).

     **@TSDIR@**
     Represents the table space directory.

     If **@TSDIR@** is omitted from data file specification of a table space, the data file is created in the database manager directory.

     **@DB_USER@**
     Represents the runtime IBM Business Monitor database user.
   - **For DB2 for z/OS**, edit the following variables:

     **@STOGRP@**
     Represents the DB2 storage group name (for example, SYSDEFLT).

     **@DB_NAME@**
     Represents the name of the IBM Business Monitor database.

     **@SCHEMA@**
     Represents the name of the IBM Business Monitor schema qualifier.

     **@DB_USER@**
     Represents the runtime IBM Business Monitor database user.
   - **For SQL Server**, edit the following variables:

     **@DB_NAME@**
     Represents the name of the IBM Business Monitor database (for example, MONITOR).

     **@SCHEMA@**
     Represents the name of the IBM Business Monitor schema (for example, MONITOR).

     **@DB_USER@**
     Represents the runtime IBM Business Monitor database user.

     **@DB_PASSWORD@**
     Represents the password of the runtime IBM Business Monitor database user. You can create the database user and password before running the script, or you can design the script to create the database user and password for you. If the script will create the database user and password, you must specify @DB_PASSWORD@ in the script.
   - **For Oracle**, edit the following variables:

**@SCHEMA@**
Represents the name of the database user that owns the IBM Business Monitor database tables.

**@DB_PASSWORD@**
Represents the password for the database user identified by $SCHEMA$.

**@TSDIR@**
Represents the table space directory.

If @TSDIR@ is omitted from the data file specification of a table space, the data file is created in the database manager directory. If a fully qualified path is specified for @TSDIR@, the directory must exist before you invoke this script.

**@DB_USER@**
Represents the runtime IBM Business Monitor database user.

The table spaces are created in the **createDatabase.sql** file. If you decide to replace the default table space names with your own table space names, when models are deployed you must export the model schema scripts and modify them to refer to your chosen table space names.

**Important:** If you are configuring an additional monitoring instance in one Oracle installation, you must also replace the string **DEFAULTTS** in createDatabase.sql with a unique identifier for this additional monitoring instance in the following four lines:

```
CREATE TABLESPACE MONDSTS
  DATAFILE 'DEFAULTTS_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
  DATAFILE 'DEFAULTTS_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
  DATAFILE 'DEFAULTTS_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
  DATAFILE 'DEFAULTTS_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
NEXT 40M MAXSIZE UNLIMITED LOGGING; ;
```

For example, if the unique identifier of the additional monitoring instance was **MONDEV1_MONDSTS**, the edited lines would look like this:

```
CREATE TABLESPACE MONDSTS
   DATAFILE 'MONDEV1_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
   DATAFILE 'MONDEV1_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
   DATAFILE 'MONDEV1_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
   DATAFILE 'MONDEV1_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
NEXT 40M MAXSIZE UNLIMITED LOGGING;
```

Repeat this procedure for each additional monitoring instance.

**Note:** Version 6.2 of IBM Business Monitor used different table spaces from previous versions. This means that if you are using Oracle and intend to deploy a 6.1 model to IBM Business Monitor 8.0, you must choose one of the following options:

– Run the 6.1 table space statements during the installation of the 8.0 database.
– When you deploy a monitor model, export the model database script and manually change the table space references to point to the 7.0 table space names. If you choose the second option, you must do this each time you deploy a 6.1 model to the 7.0 server.

A simple way to avoid this issue is to migrate from 6.1 to 8.0 with existing models deployed, and then generate new models in 6.2 or 8.0 IBM Business Monitor development toolkit.
The map of table space names is shown in the table below.

*Table 3. Map of table space names from previous versions of IBM Business Monitor*

| Current Table Space | 6.1.x Table Space |
|---|---|
| MONDSTS | INSTANCE |
| MONDMSTS | DMSTS |
| MONIDXTS | INDEXTS |
| MONLOBTS | LOBTS |

3. Save and close the file.

## Configuring COGNOSCS database scripts manually

The database scripts required for creating the COGNOSCS database for IBM Cognos Business Intelligence are shipped on the installation media and are copied to the application server during IBM Business Monitor server installation. These database scripts can be customized manually so that you can create the databases before server installation or profile creation.

To edit the database script files manually, complete the following steps:

1. Using a text editor, open the database script file for your database software.
   - For DB2 for z/OS, the `createDatabase_Cognos.sql` script creates the database.
   - For all other databases, the `createDatabase.sql` script creates the database.

   By default, the file is located in the following directories:

   app_server_root/`dbscripts/Cognos`

   app_server_root/`profiles/`*`profile_name`*`/dbscripts/Cognos`

   where

   *app_server_root* is the directory where IBM Business Monitor is installed
2. Edit the following variables in the database script files for your database software:
   - **For DB2 for z/OS**, the default schema for the database user will be used. Edit the following variables:

     **@STOGRP@**
     Represents the DB2 storage group name (for example, SYSDEFLT).

     **@COG_DB_NAME@**
     Represents the name of the IBM Business Monitor database (for example, COGNOSCS).
   - **For all other databases**, the default schema and table space for the database user will be used. Edit the following variables:

     **@COG_DB_NAME@**
     Represents the name of the IBM Business Monitor database (for example, COGNOSCS).

     **@DB_USER@**
     Represents the runtime IBM Business Monitor database user.
3. Save and close the file.
4. **For DB2 for z/OS only**:

a. On DB2 for z/OS, you must create the table spaces using the IBM Cognos BI scripts `tablespace_db2zOS.sql` and `NC_TABLESPACES.sql`. See the full instructions in the IBM Cognos BI information center:

   Suggested Settings for Creating the Content Store in DB2 on z/OS

   Create Tablespaces for a DB2 Content Store on z/OS

b. The first time IBM Cognos BI starts, it creates the tables using the following scripts:

   *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitTest_db2zOS.sql`

   *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitScript_db2zOS.sql`

   *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitLock_db2zOS.sql`

   *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitMeta_db2zOS.sql`

   *COGNOS_location*`/configuration/schemas/delivery/zosdb2/NC_CREATE_DB2.sql`

   For network deployment (ND) environments, the initial server startup will first copy these files from the master IBM Cognos BI installation location to the server location. Make sure that you have replaced the environment-specific variables in these files before the IBM Cognos BI server starts; otherwise the table creation scripts will fail when the server starts. To determine your *COGNOS_location*, see Locating your runtime IBM Cognos BI root directory.

## Installing the MONITOR database manually

You can use database scripts to install the IBM Business Monitor database manually, either on the same server as the IBM Business Monitor server or as a remote database on another server. Before running the scripts, ensure that the environment-specific variables in the scripts have been configured, either manually or using the database design tool.

Before you complete this task, make sure that you have read "Database considerations" and any prerequisites for your specific database product. For example, if you are using DB2 for z/OS, a dedicated storage group (STOGROUP) is recommended for IBM Business Monitor. The storage group must be created before the database is created.

Complete the following steps on the server where the database software is installed:

1. Log in to the database server as a user with authority to create table spaces and database objects.
2. Locate the DDL scripts.
   - If you are using the scripts that are delivered when IBM Business Monitor is installed, they are found in the **app_server_root/dbscripts/Monitor** directory.
   - If you used DbDesignGenerator to generate the scripts with your variable values substituted, they are in the output directory you chose while running the utility (by default **app_server_root/util/dbUtils**).
   - If you had profile creation generate the scripts with your variable values substituted, they are in the output directory that you chose when creating the profile (by default **app_server_root/profiles/<*profile*>/dbscripts/Monitor**).
3. From the command line interface, run the script, using the following command for your database software. The script creates the database for IBM Business Monitor.
   - **DB2**: **db2 -tf createDatabase.sql**
   - **DB2 for z/OS**:

     **db2 -tf createDatabase_Monitor.sql**

     **db2 -tf createTablespace_Monitor.sql**

     The database scripts can be run using either the SPUFI or the DSNTEP2 utility.
   - **Oracle**: **sqlplus** ***dbadmin/password @ database_name*** **@createDatabase.sql** where

     *dbadmin* is an Oracle user with administrative authority

     *database_name* is the Oracle ID (for example, **orcl**)

- **Microsoft SQL Server**: **sqlcmd -U** *dbadmin* **-P** *password* **-e -i createDatabase.sql** where
  *dbadmin* is a SQL Server user with administrative authority

4. Run the script to create tables using one of the following commands:
   - **DB2**:

     ```
     db2 connect to MONITOR
     db2 -tf createTables.sql
     db2 connect reset
     ```

     **Note:** While running the DDL file, you might see the following warning message: **SQL0347W The recursive common table expression "MON023.WBITIME" may contain an infinite loop. SQLSTATE=01605.** You can safely ignore this message.
   - **DB2 for z/OS** :

     ```
     db2 connect to MONITOR
     db2 -tf createTable_Monitor.sql
     db2 connect reset
     ```

     **Note:** While running the DDL file, you might see the following warning message: **SQL0347W The recursive common table expression "MON023.WBITIME" may contain an infinite loop. SQLSTATE=01605.** You can safely ignore this message.
   - **Oracle**: **sqlplus** *user/password@database_name* **@createTables.sql**
   - **Microsoft SQL Server**: **sqlcmd -U** *user* **-P** *password* **-e -i createTables.sql**
5. Start WebSphere Application Server.

## Installing the COGNOSCS database manually

You can use the `createDatabase` script, or, for DB2 for z/OS, the `createDatabase_Cognos` script, to install the IBM Cognos Business Intelligence content store database manually, either on the same server as the IBM Business Monitor server or as a remote database on another server. Before running the script, ensure that the environment-specific variables in the script have been configured, either manually or using the database design tool.

Before you complete this task, make sure that you have read "Database considerations" and any prerequisites for your specific database product.

Complete the following steps on the server where the database software is installed:

1. Log in to the database server as a user with authority to create table spaces and database objects.
2. Locate the DDL scripts.
   - If you are using the scripts that are delivered when IBM Business Monitor is installed, they are found in the **app_server_root/dbscripts/Cognos** directory.
   - If you used DbDesignGenerator to generate the scripts with your variable values substituted, they are in the output directory you chose while running the utility (by default **app_server_root/util/dbUtils**).
   - If you had profile creation generate the scripts with your variable values substituted, they are in the output directory that you chose when creating the profile (by default **app_server_root/profiles/<*profile*>/dbscripts/Cognos**).
3. From the command line interface, run the script, using the following command for your database software.
   - **DB2**: **db2 -tf createDatabase.sql**
   - **DB2 for z/OS**: **db2 -tf createDatabase_Cognos.sql**. The database script can be run using either the SPUFI or the DSNTEP2 utility.
   - **Oracle**: **sqlplus** *dbadmin/password @ database_name* **@createDatabase.sql** where
     *dbadmin* is an Oracle user with administrative authority

*database_name* is the Oracle ID (for example, **orcl**)

- **Microsoft SQL Server**: **sqlcmd -U *dbadmin* -P *password* -e -i createDatabase.sql** where
  *dbadmin* is a SQL Server user with administrative authority

4. **For DB2 for z/OS only**:
   a. On DB2 for z/OS, you must create the table spaces using the IBM Cognos BI scripts `tablespace_db2zOS.sql` and `NC_TABLESPACES.sql`. See the full instructions in the IBM Cognos BI information center:

      Suggested Settings for Creating the Content Store in DB2 on z/OS

      Create Tablespaces for a DB2 Content Store on z/OS

   b. The first time IBM Cognos BI starts, it creates the tables using the following scripts:

      *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitTest_db2zOS.sql`

      *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitScript_db2zOS.sql`

      *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitLock_db2zOS.sql`

      *COGNOS_location*`/configuration/schemas/content/db2zOS/dbInitMeta_db2zOS.sql`

      *COGNOS_location*`/configuration/schemas/delivery/zosdb2/NC_CREATE_DB2.sql`

      For network deployment (ND) environments, the initial server startup will first copy these files from the master IBM Cognos BI installation location to the server location. Make sure that you have replaced the environment-specific variables in these files before the IBM Cognos BI server starts; otherwise the table creation scripts will fail when the server starts. To determine your *COGNOS_location*, see Locating your runtime IBM Cognos BI root directory.

5. Start WebSphere Application Server.

## Creating messaging engine tables manually

If you did not automatically create the service integration (SI) bus tables for the IBM Business Monitor messaging engine during stand-alone profile creation, or while using the deployment environment configuration wizard or configuration wizard, you must create the tables manually. You must also create the tables manually if you are using DB2 for z/OS for the messaging engine data store.

You can also create a common event infrastructure (CEI) messaging engine table. When the deployment environment is created, the database scripts for CEI are generated. You must run the scripts manually to complete the configuration if you would like to enable the CEI event store (not recommended for production environments).

Use the database design tool (DbDesignGenerator) to generate scripts for the SI bus tables in version 8.0.

You can also use sibDDLGenerator as an alternative. For example, the command to generate SIB DDL scripts for DB2 for z/OS is **sibDDLGenerator -system db2 -version 8.1 -platform zos**.

The documentation for the sibDDLGenerator shows the versions of DB2 that are supported. It does not list all the versions of DB2 that are supported by IBM Business Monitor; however, you can specify version 8.1 as shown in the example above and the resulting DDL should be compatible with all supported versions.

Because IBM Business Monitor can have a CEI messaging engine as well as the IBM Business Monitor messaging engine, each created with the same table space and table names, ensure that you either use two different databases or two different schema names.

## Generating scripts for creating database objects in DB2 for z/OS

If you have an existing database design file, you can use it to generate database scripts for creating IBM Business Monitor database objects in a DB2 for z/OS database subsystem.

Install IBM Business Monitor.

Ensure that you have the appropriate file permissions to create the database design file and the database scripts in the intended locations.

To generate the database scripts for creating your database objects, you can run the database design tool in silent mode with the **-g** command-line parameter. In this mode, the tool requires input from a database design file that defines the configuration for your DB2 for z/OS database. The database design file must already exist before you generate the database scripts.

You can run the database design tool in interactive mode to generate a database design file. Follow the prompts in the tool to define a DB2 for z/OS database configuration for your stand-alone or network deployment topology.

While defining a DB2 for z/OS database configuration, you can specify how to group the SQL database scripts that you want to generate for the IBM Business Monitor components. The default setting is for the scripts to be generated in individual directories for each component. Before you run the database design tool, decide on a location for storing the files that the tool will generate.

It is important to use a directory path and structure that reflects how you want the database objects to be distributed across the DB2 for z/OS subsystem. For each database to be created, use a single output directory, and generate all the schema that is required to create the database, into that directory. As a reference aide, you can also base the name of the SQL directory on the name of the database that you plan to create.

For example, if you intend to create a single database called W1MYDB, you can generate the database scripts for all the database components in the single directory `WAS_HOME/profiles/default/dbscripts/DB2-zOS/W1MYDB`. If you require two databases, which are scoped at the cell level and the cluster level, you can structure the database schema as shown in the following example:

- To create a database called W8CELLDB, which contains database objects that are scoped at the cell level, generate the database scripts for the MONITOR database component in a directory such as **WAS_HOME/profiles/default/dbscripts/DB2-zOS/W8CELLDB**. You can later run the generated schema to create the database objects for the MONITOR database component in the W8CELLDB database. *
- To create a database called W8S1DB, which contains the database objects that are scoped at the cluster level, generate the database scripts for all the remaining IBM Business Monitor components in a directory such as **WAS_HOME/profiles/default/dbscripts/DB2-zOS/W8S1DB**. You can later run the generated schema to create the database objects for these components in the W8S1DB database.

1. If necessary, copy the database design file, which defines your DB2 for z/OS configuration, to the workstation where IBM Business Monitor is installed, to make the file available for use with the **DbDesignGenerator** command.
2. Change to the IBM Business Monitor directory where the **DbDesignGenerator** command is stored:

   **cd WAS_HOME/util/dbUtils**

   For example: **cd /WebSphere/V8T8DM/DeploymentManager/util/dbUtils**
3. Run the **DbDesignGenerator** command using the following syntax:

   **./DbDesignGenerator.sh -g db_design_file**

   where *db_design_file* is the fully qualified name of the database design file. For example:

   **./DbDesignGenerator.sh -g /WebSphere/V8T8DM/DeploymentManager/profiles/default/dbscripts/DB2-zOS/W8CELL.nd.dbDesign**

4. Review the information that is displayed on the screen, checking that no error messages are displayed. For each database component, the database design tool writes information messages to the screen to indicate that the scripts were generated in the directory specified in the database design file. For example, for the MONITOR database component, you see information similar to the following example:

   ```
   [info] The script(s) have been generated in
   /WebSphere/V8T8DM/DeploymentManager/profiles/default/dbscripts/DB2-zOS/W8CELLDB for MONITOR
   ```

   After the last set of scripts is generated, you see information similar to the following example:

   ```
   [info] thanks, quitting now ...
   ```

   **Tip:** In the database design file, the directories for the SQL scripts are defined by the *ddl_outDir* variable in each component section. If you want to generate the SQL scripts to a set of different directories, a quick way to do this is to manually update the values of the *ddl_outDir* variables. Then save the database design file, and run the **DbDesignGenerator** command again, as described in step 3 on page 58.

The following files are created:

- The database scripts are created in one or more specified directories. Each of the directories also contains a createDB2.sh script, which you can later run together with the database scripts to create the DB2 for z/OS database objects.
- A log file named `dbDesignGenerator.log` is created in the directory from which you ran the **DbDesignGenerator** command.

## Creating databases in the DB2 for z/OS subsystem

When you use the database design tool (**DbDesignGenerator**) to define your database configuration, you can generate the database scripts that are required for creating the databases for the IBM Business Monitor components.

You can use various tools to run these database scripts:

- When you run the database design tool to generate the database scripts, the **createDB2.sh** script is also generated. You can use **createDB2.sh** to run the database scripts.
- You can use tools such as the DB2 command line processor, SPUFI, or DSNTEP2 to run the database scripts.

### Choosing which tool to use

You can choose one tool over another based on experience and familiarity, or personal preference. Your organization might also have implemented standards or conventions for the tools used to create DB2 for z/OS objects, particularly in a production environment.

### Considerations for choosing the createDB2.sh script

- **createDB2.sh** can create all your database objects in one simple execution of the tool, so it is a good choice if this is your first server implementation.
- **createDB2.sh** runs the database scripts that the database design tool (**DbDesignGenerator**) generates.
- **createDB2.sh** runs the SQL for each component in the correct sequence.
- **createDB2.sh** creates database objects according to a naming convention that you define.
- **createDB2.sh** organizes the layout of database objects across DB2 for z/OS databases.
- **createDB2.sh** issues GRANT permissions to database, storage group, and buffer pool objects.
- **createDB2.sh** automatically completes customization of the service integration bus Data Definition Language (DDL).
- **createDB2.sh** runs in a UNIX System Services environment.

- **createDB2.sh** produces an audit trail of the objects that it creates.

### Considerations for choosing other tools

- You might prefer to use the DB2 command line processor to run the SQL statements in the UNIX Systems Services environment. You must first run the **createDB2.sh** script in a mode that bypasses execution of the SQL statements and instead consolidates them into two `.sql` files. You can then run these files by using the command line processor.
- There is no restriction on the naming or organization conventions that apply to the database objects other than the standard database subsystem restrictions.
- Some tools can be run from a z/OS environment.
- The tools can produce an audit trail of the DB2 database commands that have been issued.

## Setting up alias name definitions for connecting to the DB2 for z/OS server

Before you run the **createDB2.sh** script, you must configure the DB2 command line processor by defining a set of environment variables and a **db2** command alias. You must also define alias names that can be used to connect to the DB2 for z/OS server.

Ensure that a properties file, for example, `clp.properties`, exists for the DB2 command line processor. If required, you can create your own properties file by using the sample properties file that is available in the directory where the command line processor is installed. For more information, see your DB2 for z/OS documentation.

Complete the following configuration steps in the z/OS UNIX System Services environment from which the **createDB2.sh** script will be run:

1. Configure the DB2 command line processor for each user ID that will work with DB2 for z/OS from the command line. You can update the personal or shared user profiles as follows:
   - Modify the CLASSPATH environment variable to include the `clp.jar` file.
   - Use the CLPPROPERTIESFILE environment variable to define the fully qualified name of the properties file for the command line processor.
   - Define the **db2** command as an alias for the command that starts the command line processor.
   - Specify the `DB2JccConfiguration.properties` file that defines the JDBC properties to be applied to the command line processor.

   You can use the following syntax to add the required entries to the `.profile` or `/etc/profile` file:

   ```
   export CLPHOME=clp_install_dir
   export CLASSPATH=$CLASSPATH:$CLPHOME/lib/clp.jar
   export CLPPROPERTIESFILE=clp_properties_file_path
   alias db2="java -Ddb2.jcc.propertiesFile=
   /file_path/DB2JccConfiguration.properties com.ibm.db2.clp.db2"
   ```

   For example:

   ```
   export CLPHOME=/shared/db2910_base
   export CLASSPATH=$CLASSPATH:$CLPHOME/lib/clp.jar
   export CLPPROPERTIESFILE=/wasv8config/clp.properties
   alias db2="java -Ddb2.jcc.propertiesFile=
   /wasv8config/DB2JccConfiguration.properties com.ibm.db2.clp.db2"
   ```

2. In the properties file for the command line processor, define alias names that can be used to connect to the DB2 for z/OS server. An alias name definition includes the following entities:
   - A URL that specifies the domain name or IP address of the database server, the port on which the server listens, the DB2 location name defined during installation, and the property for the JDBC connection. The URL can take the form: *server*:*port*/*database* property=*value*. The port and property values are optional, and the DB2 location name must be specified in uppercase characters.

- A user ID and an associated password that can be used to connect to the DB2 server. This user ID should correspond to the user ID (with SYSADM authority) that the DB2 system administrator uses to run the **createDB2.sh** script.

You can add the required alias name entries to the properties file by using the following syntax:

```
DB2ALIASNAME=URL,user_ID,password
```

For example:

```
DSNXWBD=localhost:9446/DSNXWBD,SYSADM1,SYSPWRD1
```

**Tip:** When you define a *DB2ALIASNAME* value in the properties file, ensure that the correct connection details are specified to avoid connecting to the wrong database and inadvertently overwriting its contents.

3. Configure the DB2 DBACRVW subsystem parameter to enable user IDs with DBADM authority on a database to perform the following tasks for other user IDs: create views on tables in the database, create aliases for tables, and create materialized query tables. You can use the installation Command List (CLIST) to access the DSNTIPP ISPF panel and update the DBADM CREATE AUTH field to set DB2 ZPARM DBACRVW=YES.

Use the **createDB2.sh** script to either run the SQL to create the database objects for a specified database, or to consolidate the SQL statements into two `.sql` files that you can run later using other database tools.

## Creating DB2 for z/OS database objects using the createDB2.sh script

After creating the database scripts for the IBM Business Monitor components, you can run the **createDB2.sh** script to create one or more databases in the DB2 for z/OS subsystem and populate each database with objects.

You can also use tools such as the DB2 command line processor, SPUFI, or DSNTEP2 to create and populate databases.

- Decide on the DB2 for z/OS database design and configuration, including the number of databases required for the IBM Business Monitor components. For example, in a stand-alone server environment, you might decide to set up all the component databases in a single DB2 for z/OS database.
- Decide on a naming convention for the DB2 for z/OS objects, such as databases, storage groups, VSAM catalog names (VCATs), schema prefixes, buffer pools, and security IDs.
- Create the required buffer pools. For more information, see Sample DB2 commands and SQL.
- Run the database design tool (**DbDesignGenerator**) to generate the database scripts that can be used to create the database objects for the IBM Business Monitor components. Set up your database configuration so that the database design tool creates a single output directory for each database to be created, and generates all the relevant database scripts, including the **createDB2.sh** script, which are required to create the database, into that directory.
- Use FTP to transfer the database scripts, including the **createDB2.sh** script, to the z/OS system that contains the DB2 for z/OS installation. Transfer the **createDB2.sh** script as an ASCII text file, and transfer the database schema files in binary mode. Also ensure that you retain the directory structure when you transfer the files.
- Grant execute permissions to the **createDB2.sh** script.
- Create or augment the profile.
- Set up alias name definitions for connecting to the DB2 server.

The number of databases that you create for your IBM Business Monitor installation can depend on your topology, and how you want to distribute your database objects across the DB2 for z/OS subsystem. Provided that the database scripts are grouped appropriately in the output directories that were specified when you ran the database design tool, you can run the **createDB2.sh** script once for each instance of a database to be created. For example:

- To create a single database, you can run **createDB2.sh** once from a directory that contains all the database scripts that were generated for all the IBM Business Monitor components.
- To create multiple databases at the cell level and cluster levels, you can run **createDB2.sh** once from each directory that contains the database scripts required to create the database objects for the cell and clusters.

**Important:** It is anticipated that the DB2 for z/OS system administrator will run the **createDB2.sh** script with a user ID that has SYSADM authority, to create the databases and storage groups. On completion, the system administrator can then grant DBADM authority for the IBM Business Monitor databases to the WebSphere administrator.

Complete the following steps for each database that you want to create:

1. In the z/OS system that contains the DB2 installation, access the UNIX System Services command shell and then change to the directory to which you transferred the database scripts for the database objects to be created. For example:

   ```
   cd /u/work/S4CELLDB
   ```

2. Run the **createDB2.sh** script by using the following syntax:

   ```
   createDB2.sh -DBAlias alias_name -DBName database_name -DBSto storage_group_name -DBCreate
   -DBVCat volume_catalog -DBUser DB_user_ID -RunSQL
   ```

   where:

   **-DBAlias**
   Specifies an alias name, which maps to the DB2 server URL, user ID, and password, and which is used to connect to DB2. If you do not specify this parameter when you run the **createDB2.sh** script, you are prompted for a value.

   **-DBName**
   Specifies the name of the database to be created.

   **-DBSto**
   Specifies the storage group name for the volumes that hold the data sets where tables and indexes are stored.

   **-DBCreate**
   Creates the database.

   **-DBVCat**
   Specifies the name of the DB2 Virtual Storage Access Method (VSAM) catalog that records information about the data sets.

   **-DBUser**
   Specifies the user ID of the WebSphere administrator that has database administration authority for the IBM Business Monitor database being created.

   **-RunSQL**
   Runs the SQL statements that create the database objects.

   For example:

   ```
   createDB2.sh -DBAlias DSNXWBD -DBName S4CELLDB -DBSto S4DBSTO -DBCreate -DBVCat DSNV10PP
   -DBUser S4ADMIN -RunSQL
   ```

   For information about all the parameters that are available for the **createDB2.sh** script and example usage, see createDB2.sh script.

3. Review the messages that are displayed in the console, checking that no error messages are displayed.

   **Tip:** The first time that you run **createDB2.sh** to create the database, you see a few messages because the script first attempts to drop the database, which at that stage does not yet exist. These messages can be ignored, and subsequent invocations of **createDB2.sh** for the same database will not produce such messages.

When the script has finished running, you can also review the `z_output.txt` file, which provides an audit trail of the operations completed and status messages. This file is stored in the directory from which you ran the **createDB2.sh** script.

Each database is created and populated with the required database objects.

## Creating DB2 for z/OS database objects using the DB2 command line processor

When you run the **createDB2.sh** script, you can choose to run the SQL immediately to create the database objects for the specified database, or you can bypass execution of the SQL scripts so that you can run them later. If you bypass execution of the SQL, the **createDB2.sh** script consolidates the SQL statements into two files (`z_schema.sql` and `z_schemaProc.sql`) that you can run later by using the DB2 command line processor.

You can also run these `.sql` files by using any other database tool of your choice, such as SPUFI or DSNTEP2.

- Decide on the DB2 for z/OS database design and configuration, including the number of databases required for the IBM Business Monitor components. For example, in a stand-alone server environment, you might decide to set up all the component databases in a single DB2 for z/OS database.
- Decide on a naming convention for the DB2 for z/OS objects, such as databases, storage groups, VSAM catalog names (VCATs), schema prefixes, buffer pools, and security IDs.
- Create the required buffer pools. For more information, see Sample DB2 commands and SQL.
- Run the database design tool (**DbDesignGenerator**) to generate the database scripts that can be used to create the database objects for the IBM Business Monitor components. Set up your database configuration so that the database design tool creates a single output directory for each database to be created, and generates all the relevant database scripts, including the **createDB2.sh** script, which are required to create the database, into that directory.
- Use FTP to transfer the database scripts, including the **createDB2.sh** script, to the z/OS system that contains the DB2 for z/OS installation. Transfer the **createDB2.sh** script as an ASCII text file, and transfer the database schema files in binary mode. Also ensure that you retain the directory structure when you transfer the files.
- Grant execute permissions to the **createDB2.sh** script.
- Create or augment the profile.
- Set up alias name definitions for connecting to the DB2 server.

Provided that the database scripts are grouped appropriately in the output directories that were specified when you ran the database design tool, you can run the **createDB2.sh** script once for each instance of a database to be created.

**Important:** It is anticipated that the DB2 for z/OS system administrator will run the **createDB2.sh** script with a user ID that has SYSADM authority, to create the databases and storage groups. On completion, the system administrator can then grant DBADM authority for the IBM Business Monitor databases to the WebSphere administrator.

Complete the following steps for each database that you want to create:

1. In the z/OS system that contains the DB2 installation, access the UNIX System Services command shell and then change to the directory to which you transferred the database scripts for the database objects to be created. For example:

   ```
   cd /u/work/S4CELLDB
   ```

2. Run the **createDB2.sh** script by using the following syntax:

   ```
   createDB2.sh -DBAlias alias_name -DBName database_name -DBSto storage_group_name -DBCreate
   -DBVCat volume_catalog -DBUser DB_user_ID
   ```

where:

**-DBAlias**
Specifies an alias name, which maps to the DB2 server URL, user ID, and password, and which is used to connect to DB2. If you do not specify this parameter when you run the **createDB2.sh** script, you are prompted for a value.

**-DBName**
Specifies the name of the database to be created.

**-DBSto**
Specifies the storage group name for the volumes that hold the data sets where tables and indexes are stored.

**-DBCreate**
Creates the database.

**-DBVCat**
Specifies the name of the DB2 Virtual Storage Access Method (VSAM) catalog that records information about the data sets.

**-DBUser**
Specifies the user ID of the WebSphere administrator that has database administration authority for the IBM Business Monitor database being created.

**Tip:** By omitting the **-RunSQL** parameter, you bypass the execution of the SQL statements that create the database objects, and instead consolidate the statements into two `.sql` files.

For example:

`createDB2.sh -DBAlias DSNXWBD -DBName S4CELLDB -DBSto S4DBSTO -DBCreate -DBVCat DSNV10PP -DBUser S4ADMIN` For information about all the parameters that are available for the **createDB2.sh** script and example usage, see createDB2.sh script.

The `z_schema.sql` and `z_schemaProc.sql` files, which hold the consolidated SQL statements, are generated in the directory from which you ran the **createDB2.sh** script. The `z_schemaProc.sql` file contains SQL statements for stored procedures, and is generated in addition to `z_schema.sql` because stored procedures require the "at" sign (@) as a statement termination character when running the command line processor.

3. Run the DB2 command line processor in batch mode to run the SQL in the `z_schema.sql` file:

   `db2 -f /`*`createDB2.sh_path`*`/z_schema.sql`

   For example:

   `db2 -f /u/work/S4CELLDB/z_schema.sql` The command line processor reads the data in the file, and processes the commands in the file consecutively.

4. Run the DB2 command line processor again to run the SQL in the `z_schemaProc.sql` file, and additionally use the **-td** parameter to define @ as the statement termination character:

   `db2 -td@ -f /`*`createDB2.sh_path`*`/z_schemaProc.sql`

   For example:

   `db2 -td@ -f /u/work/S4CELLDB/z_schemaProc.sql`

Each database is created and populated with the required database objects.

## Considerations for HADR setup and configuration

Review the following considerations while you plan to set up and configure DB2 for high availability disaster recovery (HADR).


- "Verify status of databases for takeover" on page 65
- "Configure data sources for HADR" on page 65

- "Set up programmatic transaction retry properties"
- "Specify user roles for HADR" on page 66
- "Start the messaging engine after the takeover" on page 66
- "Access additional information" on page 66


## Verify status of databases for takeover

When a site failure occurs, HADR enables the standby database to take over as the primary database, with full DB2 functionality. Before the takeover occurs, verify the DB2 HADR status of both the primary database and the standby database to see if the takeover is allowed or if an error is returned. Sometimes, the takeover might cause an error or might not be allowed.

For more information, see the TAKEOVER HADR command topic. Review the command parameters and the usage notes to determine whether to perform the takeover.

## Configure data sources for HADR

Configure the DB2 data sources for HADR in the IBM Business Manager admin console, as described in the Configuring client reroute for applications that use DB2 databases topic.

Keep in mind the following considerations when you configure the data sources for IBM Business Process Manager products:

- It is recommended to enable the automatic client reroute when setting up DB2 HADR.
- For messaging engine and cell level data sources, the *Alternate server names* and *Alternate port numbers* properties must be configured.
- The alternate port must be the external port for the DB2 server, not the HADR service port that is specified in `/etc/services`. For example, if the HADR service port `DB2_HADR_1`, specified in `/etc/services`, is `55001`, and the DB2 server uses the external port `50000`, you must specify port `50000` for the data source alternate port in the admin console.

## Set up programmatic transaction retry properties

To support programmatic transaction retries, two new properties have been added to the `00static.xml` file, with the following values:

```
<transaction-reroute-retries>3</transaction-reroute-retries>
<transaction-reroute-retry-delay-in-millis>10000<transaction-reroute-retry-delay-in-millis>
```

Use the `100Custom.xml` configuration file to customize the changes in `00Static.xml` if values other than default are required. Complete the following steps:

1. Locate `100Custom.xml` configuration file:
   - For a network deployment environment, the file path is `<DMGR-profile-root>\config\cells\<cell-name>\nodes\<custom-node-name>\servers\<server-name>\server_type\config\100Custom.xml`.
   - For a stand-alone server environment, the file path is: `<stand-alone-profile-root>\config\cells\<cell-name>\nodes\<stand-alone-node-name>\servers\<server-name>\server_type\config\100Custom.xml`.
2. Edit the `100Custom.xml` file. Edit the following section to look like this example:

   ```
   CEI61Configur E
   com.ibm.wbimonitor.observationmgr.spi.impl.CEI61RemoteConfigurationSessionImpl reloadCEIConfig(String[]
   eventServerAppNames) CWMRT7314E: Error while trying to reload the CEI configuration.
   ```
3. Save your changes.

Provide all the client reroute properties for all your data sources.

### Specify user roles for HADR

When setting up HADR, specify appropriate user roles per platform to determine who can perform different HADR tasks.

- For Windows, use the DB2 administrative user: `db2admin`
- For Linux, use the DB2 instance user, `db2inst1`, rather than the administrative user, `dasusr1`.

For example, if the DB2 instance user is specified, the `db2inst1` user backs up the primary database, copies the backup image to the standby server, and then restores or starts the standby server using this image. If the administrative user is specified, the `dasusr1` user is the owner of the copied image, which the `db2inst1` user who performs the backup and restore actions cannot access. Because the two users belong to different groups and have different access rights to files, the HADR setup might fail.

### Start the messaging engine after the takeover

If the auto restart for the messaging engine is disabled, you must manually start the messaging engine after the database takeover occurs.

When two messaging engine servers exist in the same cluster, with messaging server 1 in an active state and messaging engine server 2 in a joined state, you might not have a running messaging engine server in your environment because of the following sequence of events:

1. The database that the messaging engines use has been taken over.
2. Messaging engine server 1 shut down to prevent data loss.
3. Messaging engine server 2 started all the messaging engines and is working as the active server while the messaging engine server 1 is still down.
4. Another takeover of the database occurred.
5. Messaging engine server 2 shut down to prevent data loss.
6. Both messaging engine servers 1 and 2 are down.

### Access additional information

If more information is needed, use the following links.

- If an outage occurs in your DB2 HADR environment, see Detecting and responding to system outages in a high availability solution.
- After the failover occurs, if the DB2 HADR status is not `peer` and if some data loss occurs, configure the DB2 HADR status to `peer` as described in the following topics:
  - Performing an HADR failover operation
  - Reintegrating a database after a takeover operation

## Configuring Oracle Real Application Cluster (RAC) for use with IBM Business Monitor

Oracle Real Application Clusters (RAC) is an option of an Oracle database that brings together two or more computers to form a clustered database that behaves as a single system. In a RAC database, Oracle processes that are running in separate nodes access the same data from a shared disk storage.

When you create IBM Business Monitor profiles using Oracle, enter the host and port of one of the RAC servers and the service name of the RAC service for the database name.

Then, after the systems are running, complete the configuration steps to modify the WebSphere data sources that should connect to the Oracle RAC with the RAC service name.

Depending on the version of Oracle RAC you are using with IBM Business Monitor, you might have to complete some configuration steps.

- If you are using Oracle 11g R2 with the SCAN feature, IBM Business Monitor does not need additional manual configuration if you specify the service name during profile creation or topology configuration. **jdbc:oracle:thin:@//[SCAN_LISTENER_HOST][:SCAN_LISTENER_PORT]/SERVICE** is the format of the JDBC URL generated during configuration and will work for Oracle RAC without any manual updates.
- If you do not want to use the SCAN feature or are using an earlier version of Oracle that does not support the SCAN feature, you must follow the configuration steps in the procedure to configure IBM Business Monitor for use with Oracle RAC.

  There are two scenarios to consider:

  – If you are using a Standalone profile, you need to create the profile using SID as the value for the database name.
  – If you are setting up a Network Deployment environment, the profiles and the clusters need to be configured using SID.

  IBM Business Monitor always creates the JDBC URL in the following format:

  ```
  jdbc:oracle:thin:@//[SCAN_LISTENER_HOST][:SCAN_LISTENER_PORT]/SERVICE
  ```

  You can edit that format for use with Oracle RAC:

  ```
  jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=
  (ADDRESS=(PROTOCOL=TCP)(HOST=rac-node1)(PORT=1521))
  (ADDRESS=(PROTOCOL=TCP)(HOST=rac-node2)(PORT=1521))
  (FAILOVER=on)(LOAD_BALANCE=on)
  (CONNECT_DATA=(SERVER=DEDICATED)
  (SERVICE_NAME=service_name)))
  ```

Specify the RAC URL as the Oracle URL when defining the relevant Oracle JDBC data sources:

1. In the administrative console, select **Resources** > **JDBC** > **Data sources**.
2. Edit all of the data sources using Oracle with the JDBC URL to use one of the formats shown in "About this task".

If you are using IBM Cognos BI, after the systems have been restarted and are functioning, the IBM Business Monitor cubes can be published. When the first cube is published, the **WBMONITOR_DB** data source is created in IBM Cognos BI using the Oracle RAC URL that is now being used by the WebSphere data source.

If the cubes were published before the change in the Oracle RAC URL, complete the following steps:

1. In IBM Cognos BI, use **IBM Cognos Administration** to remove the **WBMONITOR_DB** data source.
2. Republish the cubes to re-create the IBM Cognos BI connection using the Oracle RAC URL.

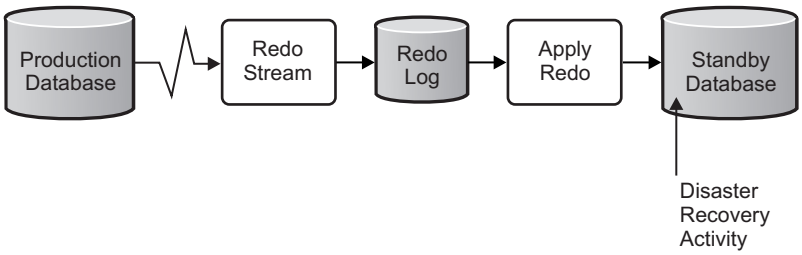
## Configuring Oracle Data Guard for IBM Business Monitor

You can configure Oracle Data Guard to be used with IBM Business Monitor. Oracle Data Guard provides high availability, disaster recovery, and data protection and is used to create, manage, and monitor one or more standby databases so that production Oracle databases can survive disasters and data corruptions.

When IBM Business Monitor is configured to use Oracle Data Guard, you typically have one production database, which is your primary database, and several standby databases. Then Oracle Data Guard automatically maintains each standby database by transmitting redo data from the primary database and applying the redo data to the standby database. If your production database becomes unavailable because of a planned or an unplanned outage, Oracle Data Guard enables you to switch any standby database to the production role, minimizing the downtime that is associated with the outage.

Oracle Data Guard automatically maintains each standby database by transmitting redo data from the primary database and then applying the redo to the standby database.

**A Typical Data Guard Configuration**




1. Set up the Oracle Data Guard environment.
2. Create a database service from the primary database:
   ```
   Exec DBMS_SERVICE.CREATE_SERVICE('BPM','BPM');
   ```
3. Create a trigger from the primary database by running the following command:
   ```
   CREATE OR REPLACE TRIGGER START_SERVICES AFTER STARTUP ON DATABASE DECLARE ROLE VARCHAR(30);
   BEGIN SELECT DATABASE_ROLE INTO ROLE FROM V$DATABASE; IF ROLE = 'PRIMARY' THEN
   DBMS_SERVICE.START_SERVICE('BPM'); END IF;END
   ```

   **Note:** When you start a database, your primary database always starts a BPM service. Therefore, your client always connects to the primary database.
4. Restart the primary database or start the following service by running the following command:
   ```
   EXEC DBMS_SERVICE.START_SERVICE('BPM');
   ```
5. Install the IBM Business Monitor.
6. Create profiles or a deployment environment that is similar to that of an Oracle instance database. While creating the profile, select **Oracle database** and connect to the database service that you created in step 2.

If all your primary and the standby databases are installed on the same server, the databases share the same IP address and Oracle listening port. No further configuration is required.

However, if your primary and standby databases are installed on different servers, they will have different IP addresses and the same Oracle listening port. If your primary and standby databases are on separate servers, you must modify all data sources, after which you will have a JDBC URL that resembles the following URL:

To modify the JDBC URL:

1. Log in to the IBM Business Monitor administrative console.
2. Go to **Resources** > **JDBC** > **Data sources**.
3. Modify all data sources that connect to the Oracle database with the URLs that resemble the following URL:
   ```
   jdbc:oracle:thin:@(DESCRIPTION=
   (ADDRESS_LIST=
   (ADDRESS=(PROTOCOL=TCP)(HOST=<host A>)(PORT=1521))
   (ADDRESS=(PROTOCOL=TCP)(HOST=<host B>)(PORT=1521))
   (ADDRESS=(PROTOCOL=TCP)(HOST=<host C>)(PORT=1521))
   (LOAD_BALANCE=off)
      (FAILOVER=on)
     )
              (CONNECT_DATA=(SERVICE_NAME=BPM))
    )
   ```

# Chapter 6. Creating and augmenting profiles

After you have installed IBM Business Monitor, create at least one profile to prepare your runtime environment. You can create and augment profiles either through the Profile Management Tool or through the **manageprofiles** command.

If you are using Solaris in 64-bit mode, the Profile Management Tool user interface is not available. You must use the **manageprofiles** command. If you are using z/OS, you cannot use either the command or the Profile Management Tool. See "Creating common configurations for IBM Business Monitor for z/OS" instead.

There are three types of profiles: a stand-alone server profile, a deployment manager profile (a management profile with a deployment manager server), and a custom profile (managed node). Each profile defines a separate runtime environment, with separate files (commands, configuration files, and log files).

## Creating and augmenting profiles using the Profile Management Tool

The Profile Management Tool in the WebSphere Customization Toolbox lets you create or augment profiles to manage your runtime environment.

**Restriction:** If you are using Solaris in 64-bit mode, the Profile Management Tool user interface is not available. You must use the **manageprofiles** command. If you are using z/OS, see "Creating common configurations for IBM Business Monitor for z/OS."

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

For a single-server environment, create a stand-alone profile.

For a network deployment environment, complete the following steps:

1. Create the deployment manager profile before creating the other profiles. If you created a deployment manager profile before installing IBM Business Monitor (for example, for WebSphere Application Server or Process Server) and you plan to use the same deployment manager profile to manage IBM Business Monitor nodes, augment the profile using the template that IBM Business Monitor provides.
2. Create a custom profile for each node that you plan to add to the server cluster. Alternatively, augment an existing custom profile for each node that you plan to add.

   **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

If you are using an Oracle database, JDBC support is provided by the Oracle JDBC drivers for JVM 1.6. The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application

© Copyright IBM Corp. 2005, 2012

Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.

By default, the Profile Management Tool points to the `ojdbc6.jar` file supplied in **app_server_root\jdbcdrivers\Oracle**. Alternatively, you can download another Oracle `ojdbc6.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command.

If you are using an SQL Server database, the SQL Server JDBC drivers for JVM 1.6 provide JDBC support. IBM Business Monitor uses the Microsoft JDBC 2.0 driver `sqljdbc4.jar` file. By default, the Profile Management Tool points to the `sqljdbc4.jar` file supplied in **app_server_root\jdbcdrivers\SQLServer**. Alternatively, you can download another Microsoft `sqljdbc4.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command. For information about minimum required settings for SQL Server, see the related link.

## Creating stand-alone profiles

If you have not created the IBM Business Monitor profile during a single-server installation, you must create the profile. The profile will be created in the WebSphere Application Server profiles directory.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

Complete the following steps to create a stand-alone application server profile using the Profile Management Tool:

1. Open the Profile Management Tool using one of the following methods:
   - From the IBM Business Monitor First Steps console, click **Profile Management Tool**.
   - Windows Click **Start** > **Programs** > **IBM** > **Business Monitor 8.0** > **Profile Management Tool**.
   - Windows Run `pmt.bat`, which is located in the following directory: **app_server_root\bin\ProfileManagement**
   - Linux UNIX Change to the **app_server_root/bin/ProfileManagement** directory and type **./pmt.sh** in a terminal window.
2. On the Welcome to the Profile Management Tool panel, review the information, and click **Launch Profile Management Tool**.
3. On the Profiles panel, click **Create** to create a new profile.
4. On the Environment Selection panel, expand IBM Business Monitor, click **Stand-alone monitor server**, and click **Next**.

   **Restriction:** If you cannot see the IBM Business Monitor option, it might indicate that you are using Solaris in 64-bit mode. In that case, you cannot use the Profile Management Tool and must use the **manageprofiles** command.

5. On the Profile Creations Options panel, select the type of installation you want to perform and click **Next**.
   - **Typical profile creation** (default): Creates the IBM Business Monitor profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, and cell. The tool also installs the administrative console, installs default applications, and assigns unique port values. You can choose to enable administrative security during the configuration. Depending on the operating system and your user permissions, the tool might create a system service to run IBM Business Monitor.
   - **Advanced profile creation**: Creates the IBM Business Monitor profile using default configuration settings, or you can select your own IBM Business Monitor components. You can assign your own port values. You can choose to deploy the administrative console, deploy sample applications, and create a web server definition. Depending on the operating system and your user permissions, you might choose to run IBM Business Monitor as a system service. You can determine the IBM Business Monitor model configuration. You can specify a database design file or assign your own values for the IBM Business Monitor database configuration. You can choose the IBM Cognos BI configuration for multidimensional data analysis.
6. If you selected **Typical profile creation**, skip to Step 11: Administrative Security panel.
7. Advanced: On the Optional Application Deployment panel, select **Deploy the administrative console** and **Deploy the default application**. The default application is a WebSphere Application Server application. Click **Next**.
8. Advanced: On the Profile Name and Location panel, accept the default name and location, or specify a profile name and directory path to contain the files for the runtime environment, such as commands, configuration files, and log files. The default profile name is **WBMon01**. On Windows, a typical profile directory is `C:\IBM\WebSphere\AppServer\profiles\WBMon01`.
9. Advanced: If you want to use the profile you are creating as the default profile, select **Make this profile the default**. Click **Next**.
10. Advanced: Set a performance tuning level appropriate for the profile you are creating. This parameter is a WebSphere Application Server parameter. For more information, see Tuning the application server in the WebSphere Application Server information center.
11. Advanced: On the Node and Host Names panel, enter new values or accept the default values, and click **Next**.
    - The node name is used for administration. If the node is federated, the node name must be unique within the cell.
    - The server name is a logical name for the IBM Business Monitor server.
    - The host name is the domain name system (DNS) name (short or long) or the IP address of this computer.
    - The cell name is a logical name for the group of nodes administered by this deployment manager.
12. On the Administrative Security panel, select one of the following options and click **Next**.
    - To enable security, select the **Enable administrative security** check box and enter the user name and password information.
    - To disable security, clear the **Enable administrative security** check box.

    For information about whether to enable security, see Administrative security in the WebSphere Application Server information center.

    If you selected **Typical profile creation**, skip to Step 21: Database Configuration panel.
13. Advanced: On the Security Certificate (Part 1) panel, choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, click **Next** to proceed to the verification page. To import existing certificates from keystores, browse to the certificates and then click **Next** to proceed to the verification page.
14. Advanced: On the Security Certificate (Part 2) panel, modify the certificate information to create new certificates during profile creation. If you are importing existing certificates from keystores, use the information to verify that the selected certificates contain the appropriate information. If the selected

certificates do not, click **Back** to import different certificates. You should change the default keystore password to protect the security of the keystore files and SSL certificates. For more information on securing communications between a server and a client, see Securing communications in the WebSphere Application Server information center.

15. Advanced: On the Port Values Assignment panel, review the ports that will be assigned during profile creation. You might want to keep track of these port values. Accept the given values or specify alternate port numbers and click **Next**.

16. Windows Advanced: On Windows systems, the Windows Service Definition panel is displayed. The option to **Run the Application Server process as a Windows service** is enabled by default and is configured to use local system account information to log on. Accept the default Windows service settings or disable the option, and click **Next**. To change the Windows service log on information, select the **Log on as specified user account** option and enter the user name and password for the alternate account.

    The Windows service **Startup type** is set to **Automatic** by default. You can optionally change the **Startup type** to **Manual** or **Disabled** using the list.

    Because services are global settings on Windows operating systems, any profile could start the service and as a result, you could lose track of which profile issued, for example, a "startServer" command. To avoid potential service request conflicts between different profiles, disable the **Run the Application Server process as a Windows service** option.

17. Advanced: On the web Server Definition panel, select one of the following options:

    - If you want to create a web server definition, enable the **Create a Web server definition** option. Accept the subsequent web server information that is provided or make modifications as needed.

      **Web server type**
      Options include IBM HTTP Server, Microsoft Internet Information Services, Sun Java™ System, Lotus® Domino® Web Server, and Apache Web Server.

      **web server operating system**
      Options include Windows, AIX, Solaris, and z/OS.

      **Web server name**
      Enter a name for the Web server. The default name is "webserver*1*".

      **Web server host name or IP address**
      Enter the host name or IP address of the Web server. The local host name appears by default.

      **Web server port (Default 80)**
      Enter the web server port number or accept the default (80).

    - If you do not want to create a web server definition, clear the **Create a web server definition** check box.

    web server definitions define an external Web server to WebSphere Application Server, enabling you to manage web server plug-in configuration files for the web server and in some cases to manage the web server. If you have not installed a web server or want to do this step later, you can easily do this step from the administrative console.

18. Advanced: If you chose to create a web server definition on the previous panel, enter a path for the web server installation directory and for the web server plug-in installation directory on the web Server Definition (Part 2) panel.

19. Advanced: On the IBM Business Process Manager Monitor Models panel, select **Deploy IBM Business Monitor global process monitor model** to install and configure the global process monitor model application. This model enables you to monitor BPEL or BPMN processes running on IBM Business Process Manager without generating and deploying monitor models.

20. Optional: Advanced: Configure the databases using a design file.

    a. Select **Use a database design file for database configuration** if you would like to use a design file instead of specifying the database parameters in the following panels.

b. Click **Browse**.
c. Specify the fully qualified path name for the design file.
d. Click **Next**.
e. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure local databases automatically or create tables in existing databases during profile creation. Local databases are created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

   **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating or configuring database scripts using the database design tool."

21. On the Database Configuration panel, verify your MONITOR database configuration information:
    a. For **Database product**, select your database from the list.
    b. To specify a destination directory for generated scripts, enable the **Override the destination directory for generated scripts** option and enter the path in the **Database script output directory** field. (The default directory is **monitor_root**\profiles\WBMon*01*\dbscripts\Monitor*platform*\.)
    c. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure local databases automatically or create tables in existing databases during profile creation. Local databases are created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

       **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.
    d. In the **Database name** field, enter the database name or accept the default (MONITOR).
    e. In the **Schema name** field, enter the schema name or accept the default (MONITOR). If you are using DB2 on z/OS, the IBM Business Monitor database schema name must be different from the Process Server common database schema name to prevent collisions between database objects.
    f. Click **Next**.
22. Complete the following steps on the Database Configuration (Part 2) panel. The options will vary depending on what database product you selected on the previous panel:
    a. Type *user_name* for the **User name** to authenticate with the database. This value represents an existing user ID with read and write permissions to MONITOR tables.

       **Note:** If you are using an Oracle database, this field is not editable.
    b. Type *password* for the **Password** for database authentication. This value represents the password for the specified database user ID.
    c. Type *password* in the **Confirm password** field. This value must match the value for **Password**.
    d. Browse to or enter a path for the JDBC driver classpath files. The JDBC drivers for DB2, Oracle, and SQL Server are located in **monitor_root/jdbcdrivers**.The default JDBC driver classpath is set

to use the product-specific files within this directory based on the database type that you selected on the Database Configuration panel. Alternatively, click **Browse** to enter a path to the JDBC driver classpath files.

- DB2 database: The following directory is created by default:
  `monitor_root/jdbcdrivers/DB2`
- Oracle database: The following directory is created by default:
  `monitor_root/jdbcdrivers/Oracle`

  The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.
- SQL Server database: The following directory is created by default:
  `monitor_root/jdbcdrivers/SQLServer`

  The `sqljdbc4.jar` JDBC driver file is the Microsoft SQL Server 2.0 JDBC driver. For information about minimum required settings for SQL Server, see the related link.

e. Select one of the following options for the JDBC driver type:
   - For Oracle databases:
     - **OCI**: The OCI driver requires a local Oracle client installation.
     - **Thin**: The Thin driver uses Java to communicate with the database and does not require a client on the local system.
   - For DB2 databases, profiles of IBM Business Monitor on operating systems other than z/OS are created with type 4 drivers, and profiles on z/OS are created with type 2 drivers. You can change the type after profile creation by editing the data source properties in the administrative console. A type 2 driver is a native-API driver and requires the installation of database software or a database client on the local system. A type 4 driver is a pure-Java implementation and typically provides the best performance. For the MONITOR database, no database software or clients are required on the local system.

f. Type *host_name* for the **Database server host name or IP address**. The default value is **localhost** or the fully qualified local host name if defined, and you should use this value for a single-server installation. If your database is on a remote server, you must type the fully qualified host name or IP address.

   **Note:** Except for a single-server installation, do *not* use the value `localhost` since the cluster members depend on the actual host name or IP address.

g. Type *port_number* for the **Database TCP/IP service port or listener port**. This value represents the port where the TCP/IP service is assigned or the port on which the database is listening.

h. Optional: If you are using a DB2 on z/OS database, type *subsystem_name* for the **Subsystem name**. This value is the location of the DB2 for z/OS database. No spaces are allowed in the name.

i. If you are using Oracle or SQL Server and you chose to create the database automatically, enter the following information:
   - *system_user_name* for the **Database administrator user name**. This value is the name of the database administrator for Oracle or SQL Server. This user must have access to create and drop databases and users.
   - *password* for the **Password**. This value is the password for the system administrator that is specified in the previous field.
   - *password* in the **Confirm password** field.

j. Click **Next**. If the MONITOR database has not yet been created, you will see a warning message. Click **Yes** to continue. You can create the database at a later time.

23. On the IBM Cognos BI Configuration panel, configure IBM Cognos BI for multidimensional data analysis from your dashboards.
    - To deploy IBM Cognos BI, click **Create a new Cognos server configuration** and provide the name of a database to be used for the IBM Cognos BI content store. The default name is COGNOSCS. On Oracle, the database name is the Oracle service name. On Microsoft SQL Server, the database name must be different from the MONITOR database name.

      Provide a database user name and password. If you use the same user name for the content store as for the MONITOR database, you must use the same password. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

      You must also provide the IBM Cognos BI administrator user name and password.

      **Note:** The user name and password for the IBM Cognos BI content store database are kept in the Cognos_JDBC_Alias, which allows all database credentials to be maintained in one place. Whenever you start the IBM Business Monitor IBM Cognos BI server, the current values are passed to the IBM Cognos BI configuration to allow IBM Cognos BI access to the content store. Because of this integration, you cannot change the content store user name and password using the IBM Cognos BI Configuration application.
    - If you want to use an existing version of IBM Cognos BI, click **Use an existing Cognos server configuration** and provide the external dispatcher URI of the IBM Cognos BI server. You can find this URI in the IBM Cognos BI configuration client in **Local Configuration** > **Environment** > **Dispatcher Settings** (for example, `http://my_host:my_port/p2pd/servlet/dispatch/ext`). If administrative security is enabled on the IBM Cognos BI server, you must also provide the IBM Cognos BI administrator user name and password.

      The IBM Cognos BI server does not have to be available to set this value. The server is required when you install monitor models if you want to perform multidimensional analysis for those models.
24. On the Profile Creation Summary panel, review the information. If you need to make any modifications, click **Back** and make changes as necessary.
25. Click **Create** to create the profile.
26. On the Profile Creation Complete panel, review the information about the completed profile creation.
27. Optional: Access First Steps.
    - Windows Select the **Launch the IBM Business Monitor first steps** option.
    - Linux UNIX Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
28. Click **Finish** to exit the Profile Management Tool.

During profile creation, you set port values for all required ports. If you decide to change the ports after installation, you must re-configure all port values for IBM Business Monitor to work properly.

## Creating deployment manager profiles

You must have a deployment manager profile to manage all federated servers in a cluster. If you are setting up a network deployment environment, create this profile first.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server
- Installed the database

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

Complete the following steps to create a deployment manager profile using the Profile Management Tool:

1. Open the Profile Management Tool using one of the following methods:
   - From the IBM Business Monitor First Steps console, click **Profile Management Tool**.
   - Windows Click **Start** > **Programs** > **IBM** > **Business Monitor 8.0** > **Profile Management Tool**.
   - Windows Run `pmt.bat`, which is located in the following directory: **app_server_root\bin\ProfileManagement**
   - Linux UNIX Change to the **app_server_root/bin/ProfileManagement** directory and type **./pmt.sh** in a terminal window.
2. On the Welcome to the Profile Management Tool panel, review the information, and click **Launch Profile Management Tool**.
3. On the Profiles panel, click **Create** to create a new profile.
4. On the Environment Selection panel, expand IBM Business Monitor, click **Monitor server deployment manager**, and click **Next**.

   **Restriction:** If you cannot see the IBM Business Monitor option, it might indicate that you are using Solaris in 64-bit mode. In that case, you cannot use the Profile Management Tool and must use the **manageprofiles** command.
5. On the Profile Creations Options panel, select the type of installation you want to perform and click **Next**.
   - **Typical profile creation** (default): Creates a deployment manager profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, host, and cell. The tool also installs the administrative console and assigns unique port values. You can choose to enable administrative security during the configuration. Depending on the operating system and your user permissions, the tool might create a system service to run the deployment manager. You can specify your own values for the IBM Business Monitor database configuration.
   - **Advanced profile creation**: Creates a deployment manager using default configuration settings. You can specify the values for host and cell, assign your own port values, and choose whether to deploy the administrative console. Depending on the operating system and your user permissions, you might have the option to run the deployment manager as a system service. You can specify a database design file or assign your own values for the IBM Business Monitor database configuration.
6. If you selected **Typical profile creation**, skip to Step 10: Administrative Security panel.
7. Advanced: On the Optional Application Deployment panel, select **Deploy the administrative console**, and click **Next**.
8. Advanced: On the Profile Name and Location panel, accept the default name and location, or specify a profile name and directory path to contain the files for the runtime environment, such as commands, configuration files, and log files. The default profile name is **Dmgr01**. On Windows, a typical profile directory is `C:\IBM\WebSphere\AppServer\profiles\Dmgr01`.
9. Advanced: If you want to use the profile you are creating as the default profile, select **Make this profile the default**. Click **Next**.

10. Advanced: On the Node, Host, and Cell Names panel, enter new values or accept the default values, and click **Next**.
    - The node name is used for administration. If the node is federated, the node name must be unique within the cell.
    - The host name is the domain name system (DNS) name (short or long) or the IP address of this computer.
    - The cell name is a logical name for the group of nodes administered by this deployment manager.
11. On the Administrative Security panel, select one of the following options and click **Next**.
    - To enable security, select the **Enable administrative security** check box and enter the user name and password information.
    - To disable security, clear the **Enable administrative security** check box.

    For information about whether to enable security, see Administrative security in the WebSphere Application Server information center.

    If you selected **Typical profile creation**, skip to Step 16: Database Configuration panel.
12. Advanced: On the Security Certificate (Part 1) panel, choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, click **Next** to proceed to the verification page. To import existing certificates from keystores, browse to the certificates and then click **Next** to proceed to the verification page.
13. Advanced: On the Security Certificate (Part 2) panel, modify the certificate information to create new certificates during profile creation. If you are importing existing certificates from keystores, use the information to verify that the selected certificates contain the appropriate information. If the selected certificates do not, click **Back** to import different certificates. You should change the default keystore password to protect the security of the keystore files and SSL certificates. For more information on securing communications between a server and a client, see Securing communications in the WebSphere Application Server information center.
14. Advanced: On the Port Values Assignment panel, review the ports that will be assigned during profile creation. You might want to keep track of these port values. Accept the given values or specify alternate port numbers and click **Next**.
15. Windows Advanced: On Windows systems, the Windows Service Definition panel is displayed. The option to **Run the Application Server process as a Windows service** is enabled by default and is configured to use local system account information to log on. Accept the default Windows service settings or disable the option, and click **Next**. To change the Windows service log on information, select the **Log on as specified user account** option and enter the user name and password for the alternate account.

    The Windows service **Startup type** is set to **Automatic** by default. You can optionally change the **Startup type** to **Manual** or **Disabled** using the list.

    Because services are global settings on Windows operating systems, any profile could start the service and as a result, you could lose track of which profile issued, for example, a "startServer" command. To avoid potential service request conflicts between different profiles, disable the **Run the Application Server process as a Windows service** option.
16. Optional: Advanced: Configure the databases using a design file.
    a. Select **Use a database design file for database configuration** if you would like to use a design file instead of specifying the database parameters in the following panels.
    b. Click **Browse**.
    c. Specify the fully qualified path name for the design file.
    d. Click **Next**.
    e. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure local databases automatically or create tables in existing databases during profile creation. Local databases are created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are

stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

**Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating or configuring database scripts using the database design tool."

17. On the Database Configuration panel, verify your MONITOR database configuration information:
    a. Select your database product from the list.
    b. To specify a destination directory for generated scripts, enable the **Override the destination directory for generated scripts** option and enter the path in the **Database script output directory** field. (The default directory is monitor_root\profiles\WBMon*01*\dbscripts\Monitor*platform*\.)
    c. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure a local database automatically or create tables in an existing one during profile creation or augmentation. A local database will be created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

       **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.
    d. In the **Database name** field, enter the database name or accept the default (MONITOR).
    e. In the **Schema name** field, enter the schema name or accept the default (MONITOR). If you are using DB2 on z/OS, the IBM Business Monitor database schema name must be different from the Process Server common database schema name to prevent collisions between database objects.
    f. Click **Next**.
18. Complete the following steps for the MONITOR database on the Database Configuration (Part 2) panel. The options will vary depending on what database product you selected on the previous panel:
    a. Type *user_name* for the **User name** to authenticate with the database. This value represents an existing user ID with read and write permissions to MONITOR tables.

       **Note:** If you are using an Oracle database, this field is not editable.
    b. Type *password* for the **Password** for database authentication. This value represents the password for the specified database user ID.
    c. Type *password* in the **Confirm password** field. This value must match the value for **Password**.
    d. Browse to or enter a path for the JDBC driver classpath files. The JDBC drivers for DB2, Oracle, and SQL Server are located in **monitor_root/jdbcdrivers**.The default JDBC driver classpath is set to use the product-specific files within this directory based on the database type that you selected on the Database Configuration panel. Alternatively, click **Browse** to enter a path to the JDBC driver classpath files.
       - DB2 database: The following directory is created by default:
         `monitor_root/jdbcdrivers/DB2`
       - Oracle database: The following directory is created by default:

`monitor_root/jdbcdrivers/Oracle`

The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.

- SQL Server database: The following directory is created by default:
  `monitor_root/jdbcdrivers/SQLServer`

  The `sqljdbc4.jar` JDBC driver file is the Microsoft SQL Server 2.0 JDBC driver. For information about minimum required settings for SQL Server, see the related link.

e. Select one of the following options for the JDBC driver type:
   - For Oracle databases:
     - **OCI**: The OCI driver requires a local Oracle client installation.
     - **Thin**: The Thin driver uses Java to communicate with the database and does not require a client on the local system.
   - For DB2 databases, profiles of IBM Business Monitor on operating systems other than z/OS are created with type 4 drivers, and profiles on z/OS are created with type 2 drivers. You can change the type after profile creation by editing the data source properties in the administrative console. A type 2 driver is a native-API driver and requires the installation of database software or a database client on the local system. A type 4 driver is a pure-Java implementation and typically provides the best performance. For the MONITOR database, no database software or clients are required on the local system.

f. Type *host_name* for the **Database server host name or IP address**. The default value is **localhost** or the fully qualified local host name if defined, and you should use this value for a single-server installation. If your database is on a remote server, you must type the fully qualified host name or IP address.

   **Note:** Except for a single-server installation, do *not* use the value `localhost` since the cluster members depend on the actual host name or IP address.

g. Type *port_number* for the **Database TCP/IP service port or listener port**. This value represents the port where the TCP/IP service is assigned or the port on which the database is listening.

h. Optional: If you are using a DB2 on z/OS database, type *subsystem_name* for the **Subsystem name**. This value is the location of the DB2 for z/OS database. No spaces are allowed in the name.

i. If you are using Oracle or SQL Server and you chose to create the database automatically, enter the following information:
   - *system_user_name* for the **Database administrator user name**. This value is the name of the database administrator for Oracle or SQL Server. This user must have access to create and drop databases and users.
   - *password* for the **Password**. This value is the password for the system administrator that is specified in the previous field.
   - *password* in the **Confirm password** field.

j. Click **Next**. If the MONITOR database has not yet been created, you will see a warning message. Click **Yes** to continue. You can create the database at a later time.

19. On the Cognos Content Store Database panel, if you do not already have an existing IBM Cognos Business Intelligence installation that you plan to use, enter the information to create the IBM Cognos BI content store database for multidimensional data analysis from your dashboards.
    a. Click **Create a new Cognos content store database**.
    b. Provide the name of a database to be used for the IBM Cognos BI content store. The default name is COGNOSCS. On Oracle, the database name is the Oracle service name. On Microsoft SQL Server, the database name must be different from the MONITOR database name.

c. Provide a user name and password for the database, and confirm the password. If you use the same user name for the content store as for the MONITOR database, you must use the same password. Because this user requires full access rights, it is a good idea to create a new database user for the content store database only.

   **Note:** The user name and password for the IBM Cognos BI content store database are kept in the Cognos_JDBC_Alias, which allows all database credentials to be maintained in one place. Whenever you start the IBM Business Monitor IBM Cognos BI server, the current values are passed to the IBM Cognos BI configuration to allow IBM Cognos BI access to the content store. Because of this integration, you cannot change the content store user name and password using the IBM Cognos BI Configuration application.

20. On the Profile Creation Summary panel, review the information. If you need to make any modifications, click **Back** and make changes as necessary.
21. Click **Create** to create the profile.
22. On the Profile Creation Complete panel, review the information about the completed profile creation.
23. Optional: Access First Steps.
    - Windows Select the **Launch the IBM Business Monitor first steps** option.
    - Linux UNIX Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
24. Click **Finish** to exit the Profile Management Tool.

During profile creation, you set port values for all required ports. If you decide to change the ports after installation, you must re-configure all port values for IBM Business Monitor to work properly.

## Augmenting deployment manager profiles

In a network deployment environment, you must have a deployment manager profile. Rather than create a new one, you can optionally augment an existing deployment manager profile to be the deployment manager profile for IBM Business Monitor.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server
- Installed the database

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

You can augment an existing WebSphere Application Server, Process Server, or WebSphere Enterprise Service Bus profile with the IBM Business Monitor template. Similarly, if you installed WebSphere Application Server and augmented the profile for IBM Business Monitor, you can augment that profile with Process Server or WebSphere Enterprise Service Bus if you choose.

Complete the following steps to augment an existing deployment manager profile using the Profile Management Tool:

1. Open the Profile Management Tool using one of the following methods:
   - From the IBM Business Monitor First Steps console, click **Profile Management Tool**.
   - Windows Click **Start** > **Programs** > **IBM** > **Business Monitor 8.0** > **Profile Management Tool**.
   - Windows Run `pmt.bat`, which is located in the following directory: **app_server_root\bin\ProfileManagement**
   - Linux UNIX Change to the **app_server_root/bin/ProfileManagement** directory and type **./pmt.sh** in a terminal window.
2. On the Welcome to the Profile Management Tool panel, review the information, and click **Launch Profile Management Tool**.
3. On the Profiles panel, select a profile from the list and click **Augment** to augment an existing profile. (You can expand a profile to see the augmentations that have already been done.) You must select an existing deployment manager profile to augment to be the IBM Business Monitor deployment manager profile.

   **Restriction:** If you cannot see the IBM Business Monitor option, it might indicate that you are using Solaris in 64-bit mode. In that case, you cannot use the Profile Management Tool and must use the **manageprofiles** command.
4. On the Augment Selection panel, click **Monitor server deployment manager** from the list, and click **Next**.
5. On the Profile Augmentation Options panel, click **Advanced profile augmentation**, and click **Next**. If you click **Typical**, some of the panels are not shown.
6. Optional: If the profile you are augmenting has security enabled, complete the following steps on the Administrative Security panel:
   a. Type *user_name* for the **User name**.
   b. Type *password* for the **Password**.
   c. Type *password* in the **Confirm password** field.
   d. Click **Next**.
7. Optional: Advanced: Configure the databases using a design file.
   a. Select **Use a database design file for database configuration** if you would like to use a design file instead of specifying the database parameters in the following panels.
   b. Click **Browse**.
   c. Specify the fully qualified path name for the design file.
   d. Click **Next**.
   e. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure local databases automatically or create tables in existing databases during profile creation. Local databases are created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

      **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

   If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating or configuring database scripts using the database design tool."
8. On the Database Configuration panel, verify your MONITOR database configuration information:

a. Select your database product from the list.
b. To specify a destination directory for generated scripts, enable the **Override the destination directory for generated scripts** option and enter the path in the **Database script output directory** field. (The default directory is monitor_root\profiles\WBMon*01*\dbscripts\Monitor*platform*\.)
c. Select **Delay execution of database scripts (must select if using a remote database)** if you do not want to create and configure a local database automatically or create tables in an existing one during profile creation or augmentation. A local database will be created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the database script output directory field on this page. If you create the scripts for Oracle, you must replace @DB_PASSWORD@ with the password for the schema name before running them.

   **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.
d. In the **Database name** field, enter the database name or accept the default (MONITOR).
e. In the **Schema name** field, enter the schema name or accept the default (MONITOR). If you are using DB2 on z/OS, the IBM Business Monitor database schema name must be different from the Process Server common database schema name to prevent collisions between database objects.
f. Click **Next**.

9. Complete the following steps for the MONITOR database on the Database Configuration (Part 2) panel. The options will vary depending on what database product you selected on the previous panel:
   a. Type *user_name* for the **User name** to authenticate with the database. This value represents an existing user ID with read and write permissions to MONITOR tables.

      **Note:** If you are using an Oracle database, this field is not editable.
   b. Type *password* for the **Password** for database authentication. This value represents the password for the specified database user ID.
   c. Type *password* in the **Confirm password** field. This value must match the value for **Password**.
   d. Browse to or enter a path for the JDBC driver classpath files. The JDBC drivers for DB2, Oracle, and SQL Server are located in **monitor_root/jdbcdrivers**.The default JDBC driver classpath is set to use the product-specific files within this directory based on the database type that you selected on the Database Configuration panel. Alternatively, click **Browse** to enter a path to the JDBC driver classpath files.
      - DB2 database: The following directory is created by default:
        `monitor_root/jdbcdrivers/DB2`
      - Oracle database: The following directory is created by default:
        `monitor_root/jdbcdrivers/Oracle`

        The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.
      - SQL Server database: The following directory is created by default:
        `monitor_root/jdbcdrivers/SQLServer`

        The `sqljdbc4.jar` JDBC driver file is the Microsoft SQL Server 2.0 JDBC driver. For information about minimum required settings for SQL Server, see the related link.
   e. Select one of the following options for the JDBC driver type:
      - For Oracle databases:

- **OCI**: The OCI driver requires a local Oracle client installation.
- **Thin**: The Thin driver uses Java to communicate with the database and does not require a client on the local system.

• For DB2 databases, profiles of IBM Business Monitor on operating systems other than z/OS are created with type 4 drivers, and profiles on z/OS are created with type 2 drivers. You can change the type after profile creation by editing the data source properties in the administrative console. A type 2 driver is a native-API driver and requires the installation of database software or a database client on the local system. A type 4 driver is a pure-Java implementation and typically provides the best performance. For the MONITOR database, no database software or clients are required on the local system.

f. Type *host_name* for the **Database server host name or IP address**. The default value is **localhost** or the fully qualified local host name if defined, and you should use this value for a single-server installation. If your database is on a remote server, you must type the fully qualified host name or IP address.

   **Note:** Except for a single-server installation, do *not* use the value `localhost` since the cluster members depend on the actual host name or IP address.

g. Type *port_number* for the **Database TCP/IP service port or listener port**. This value represents the port where the TCP/IP service is assigned or the port on which the database is listening.

h. Optional: If you are using a DB2 on z/OS database, type *subsystem_name* for the **Subsystem name**. This value is the location of the DB2 for z/OS database. No spaces are allowed in the name.

i. If you are using Oracle or SQL Server and you chose to create the database automatically, enter the following information:

   • *system_user_name* for the **Database administrator user name**. This value is the name of the database administrator for Oracle or SQL Server. This user must have access to create and drop databases and users.

   • *password* for the **Password**. This value is the password for the system administrator that is specified in the previous field.

   • *password* in the **Confirm password** field.

j. Click **Next**. If the MONITOR database has not yet been created, you will see a warning message. Click **Yes** to continue. You can create the database at a later time.

10. On the Cognos Content Store Database panel, if you do not already have an existing IBM Cognos Business Intelligence installation that you plan to use, enter the information to create the IBM Cognos BI content store database for multidimensional data analysis from your dashboards.

    a. Click **Create a new Cognos content store database**.

    b. Provide the name of a database to be used for the IBM Cognos BI content store. The default name is COGNOSCS. On Oracle, the database name is the Oracle service name. On Microsoft SQL Server, the database name must be different from the MONITOR database name.

    c. Provide a user name and password for the database, and confirm the password. If you use the same user name for the content store as for the MONITOR database, you must use the same password. Because this user requires full access rights, it is a good idea to create a new database user for the content store database only.

       **Note:** The user name and password for the IBM Cognos BI content store database are kept in the Cognos_JDBC_Alias, which allows all database credentials to be maintained in one place. Whenever you start the IBM Business Monitor IBM Cognos BI server, the current values are passed to the IBM Cognos BI configuration to allow IBM Cognos BI access to the content store. Because of this integration, you cannot change the content store user name and password using the IBM Cognos BI Configuration application.

11. On the Profile Augmentation Summary panel, review the information. If you need to make any modifications, click **Back** and make changes as necessary.

12. Click **Augment** to augment the profile.
13. On the Profile Augmentation Complete panel, review the information about the completed profile augmentation.
14. Optional: Access First Steps.
    - Windows Select the **Launch the IBM Business Monitor first steps** option.
    - Linux UNIX Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
15. Click **Finish** to exit the Profile Management Tool.

During profile creation, you set port values for all required ports. If you decide to change the ports after installation, you must re-configure all port values for IBM Business Monitor to work properly.

## Creating custom profiles for nodes

For a network deployment, you must create a custom profile for each node you plan to add to the IBM Business Monitor server cluster. The profile will be created in the WebSphere Application Server profiles directory.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server
- Ensured that the deployment manager is running.

**Tip:** If you are planning to enable security on these nodes, you should configure security before proceeding with the custom node creation. A link to detailed information for configuring security is provided below.

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

Complete the following steps to create a custom profile for each cluster member using the Profile Management Tool:

1. Open the Profile Management Tool using one of the following methods:
   - From the IBM Business Monitor First Steps console, click **Profile Management Tool**.
   - Windows Click **Start** > **Programs** > **IBM** > **Business Monitor 8.0** > **Profile Management Tool**.
   - Windows Run `pmt.bat`, which is located in the following directory: **app_server_root\bin\ProfileManagement**
   - Linux UNIX Change to the **app_server_root/bin/ProfileManagement** directory and type **./pmt.sh** in a terminal window.
2. On the Welcome to the Profile Management Tool panel, review the information, and click **Launch Profile Management Tool**.
3. On the Profiles panel, click **Create** to create a new profile.

4. On the Environment Selection panel, expand IBM Business Monitor, click **Monitor server custom profile**, and click **Next**. Creating a custom profile will allow you the flexibility to create servers and clusters as you continue setting up your environment.

   **Restriction:** If you cannot see the IBM Business Monitor option, it might indicate that you are using Solaris in 64-bit mode. In that case, you cannot use the Profile Management Tool and must use the **manageprofiles** command.
5. On the Profile Creations Options panel, select the type of installation you want to perform and click **Next**.
   - **Typical profile creation** (default): Creates a custom profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, and host. The node will be federated to an existing deployment manager.
   - **Advanced profile creation**: Creates a custom profile using default configuration settings. You can specify the values for the location of the profile and names of the profile, node, and host. The node will be federated to an existing deployment manager.
6. If you selected **Typical profile creation**, skip to Step 10: Federation panel.
7. Advanced: On the Profile Name and Location panel, accept the default name and location, or specify a profile name and directory path to contain the files for the runtime environment, such as commands, configuration files, and log files. The default profile name is **Custom01**. On Windows, a typical profile directory is `C:\IBM\WebSphere\AppServer\profiles\Custom01`.
8. Optional: Advanced: If you want to use the profile you are creating as the default profile, select **Make this profile the default**. Click **Next**.
9. Advanced: On the Node and Host Names panel, enter new values or accept the default values, and click **Next**.
   - The node name is used for administration. If the node is federated, the node name must be unique within the cell.
   - The host name is the domain name system (DNS) name (short or long) or the IP address of this computer.
10. On the Federation panel, complete the following steps to identify the deployment manager profile that you plan to use:

    **Note:** You can choose to federate the node later (using add_node) by selecting **Federate this node later**. If you select this option, all the fields are disabled. One advantage of federating later is that you might save yourself from creating a profile twice. If the node was federated during the profile creation and for some reason it failed (for example, the machine clock for the node is out of sync with that of the deployment manager), you need to create the profile again to ensure its validity. Federating the node at a later stage, therefore, provides a finer control on the federation procedure.
    a. Type ***host_name*** for the **Deployment manager host name or IP address**. This value is the fully qualified host name or IP address of the server where the deployment manager profile was created.
    b. Type ***port_number*** for the **Deployment manager SOAP port number**. The default value is 8879.
    c. Optional: If administrative security is enabled on the deployment manager, type ***user_name*** for the **User name**. The user name must be an existing WebSphere Application Server user for the deployment manager. This value is required for authentication with the deployment manager.
    d. Optional: If administrative security is enabled on the deployment manager, type ***password*** for the **Password**. This password must be the password for the *user_name* you provided.
    e. Click **Next**.
11. If you selected **Typical profile creation**, go to Step 15: Profile Creation Summary panel
12. Advanced: On the Port Values Assignment panel, review the ports that will be assigned during profile creation. You might want to keep track of these port values. Accept the given values or specify alternate port numbers and click **Next**.

13. Advanced: On the Database Configuration panel, complete the following steps:
    a. Select your database product from the drop-down list.
    b. Type or browse to the directory where the JDBC classpath files are located in the **Location (directory) of JDBC driver classpath files**.
    c. Click **Next**.
14. On the Profile Creation Summary panel, review the information. If you need to make any modifications, click **Back** and make changes as necessary.
15. Click **Create** to create the profile.
16. On the Profile Creation Complete panel, review the information about the completed profile creation.
17. Optional: Access First Steps.
    - Windows Select the **Launch the IBM Business Monitor first steps** option.
    - Linux UNIX Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
18. Click **Finish** to exit the Profile Management Tool.

During profile creation, you set port values for all required ports. If you decide to change the ports after installation, you must re-configure all port values for IBM Business Monitor to work properly.

## Augmenting custom profiles for nodes

For a network deployment, you need a custom profile for each node you plan to add to the IBM Business Monitor server cluster. Rather than create a new one, you can optionally augment an existing custom profile for each node.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server
- Ensured that the deployment manager is running.

Windows

**Important:** To install or run the Profile Management Tool on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges. Whether you are an administrative user or a non-administrative user, right-click the `pmt.bat` file and select **Run as administrator**. Alternatively, use the **runas** command at the command line. For example:

```
runas /user:ADMINNAME /env pmt.bat
```

Non-administrative users are prompted for the administrator password.

Complete the following steps to augment a profile for each cluster member using the Profile Management Tool:

1. Open the Profile Management Tool using one of the following methods:
    - From the IBM Business Monitor First Steps console, click **Profile Management Tool**.
    - Windows Click **Start** > **Programs** > **IBM** > **Business Monitor 8.0** > **Profile Management Tool**.
    - Windows Run `pmt.bat`, which is located in the following directory: **app_server_root\bin\ProfileManagement**
    - Linux UNIX Change to the **app_server_root/bin/ProfileManagement** directory and type **./pmt.sh** in a terminal window.

2. On the Welcome to the Profile Management Tool panel, review the information, and click **Launch Profile Management Tool**.
3. On the Profiles panel, select a profile from the list and click **Augment** to augment an existing profile. (You can expand a profile to see the augmentations that have already been done.) You must select an existing custom profile to augment to be the IBM Business Monitor custom profile. A custom profile will allow you the flexibility to create servers and clusters as you continue setting up your environment.

   **Restriction:** If you cannot see the IBM Business Monitor option, it might indicate that you are using Solaris in 64-bit mode. In that case, you cannot use the Profile Management Tool and must use the **manageprofiles** command.
4. On the Augment Selection panel, click **Monitor server custom profile** from the list, and click **Next**.
5. On the Profile Augmentation Options panel, click **Advanced profile augmentation**, and click **Next**. If you click **Typical**, some of the panels are not shown.
6. If you see the Federation panel, complete the following steps to identify the deployment manager profile that you plan to use:

   **Note:** If the profile was not previously federated, you will not see this panel.
   a. Type *host_name* for the **Deployment manager host name or IP address**. This value is the fully qualified host name or IP address of the server where the deployment manager profile was created.
   b. Type *port_number* for the **Deployment manager SOAP port number**. The default value is 8879.
   c. Optional: If administrative security is enabled on the deployment manager, type *user_name* for the **User name**. The user name must be an existing WebSphere Application Server user for the deployment manager. This value is required for authentication with the deployment manager.
   d. Optional: If administrative security is enabled on the deployment manager, type *password* for the **Password**. This password must be the password for the *user_name* you provided.
   e. Click **Next**.
7. On the Database Configuration panel, complete the following steps:
   a. Select your database product from the list.
   b. Type or browse to the directory where the JDBC classpath files are located in the **Location (directory) of JDBC driver classpath files**.
   c. Click **Next**.
8. Click **Augment** to augment the profile.
9. On the Profile Augmentation Complete panel, review the information about the completed profile augmentation.
10. Optional: Access First Steps.
    - Windows Select the **Launch the IBM Business Monitor first steps** option.
    - Linux UNIX Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
11. Click **Finish** to exit the Profile Management Tool.

During profile creation, you set port values for all required ports. If you decide to change the ports after installation, you must re-configure all port values for IBM Business Monitor to work properly.

## Creating and augmenting profiles using the manageprofiles command

Instead of using the Profile Management Tool, you can use the **manageprofiles** command to create profiles from the command line. If you are running Solaris in 64-bit mode, you must use the **manageprofiles** command because the Profile Management Tool is not supported. If you are using z/OS, see "Creating common configurations for IBM Business Monitor for z/OS."

**Important:** The **manageprofiles** command does not support profile augmentation using the **profileTemplate** parameter for cells in a different package.

Carefully consider the available parameters before creating or augmenting your profile. It is not simple to modify a profile after creation or augmentation.

Before completing this task, you must have completed the following tasks:

- Verified that all hardware and software prerequisites have been met
- Installed IBM Business Monitor
- Logged in to the system as a user with appropriate permissions (read, write, and execute) on the profiles directory of WebSphere Application Server

If you are using an Oracle database, JDBC support is provided by the Oracle JDBC drivers for JVM 1.6. The `ojdbc6.jar` JDBC driver file is the Oracle-supported JDBC driver for use with WebSphere Application Server version 7. The `ojdbc6.jar` file can be used for both Oracle 10g and Oracle 11g. For information about minimum required settings for Oracle, see the related link.

By default, the Profile Management Tool points to the `ojdbc6.jar` file supplied in **app_server_root\jdbcdrivers\Oracle**. Alternatively, you can download another Oracle `ojdbc6.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command.

If you are using an SQL Server database, the SQL Server JDBC drivers for JVM 1.6 provide JDBC support. IBM Business Monitor uses the Microsoft JDBC 2.0 driver `sqljdbc4.jar` file. By default, the Profile Management Tool points to the `sqljdbc4.jar` file supplied in **app_server_root\jdbcdrivers\SQLServer**. Alternatively, you can download another Microsoft `sqljdbc4.jar` JDBC driver file and point to it when you run the Profile Management Tool or the **manageprofiles** command. For information about minimum required settings for SQL Server, see the related link.

Windows

**Important:** To install or run the **manageprofiles** command on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges using the **runas** command. Remember to put double quotation marks around the **manageprofiles** command and all parameters. For example:

```
runas /env /user:MyAdminName "manageprofiles.bat -create -profileName WBMON01
-templatePath C:/WAS80/profileTemplates/wbmonitor/default
-wbmDBJDBCClasspath C:\IBM\WebSphere\MonServer\jdbcdrivers\DB2"
```

Non-administrative users are prompted for the administrator password.

For a single-server environment, create a stand-alone profile.

For a network deployment environment, complete the following steps:

1. Create the deployment manager profile before creating the other profiles. If you created a deployment manager profile before installing IBM Business Monitor (for example, for WebSphere Application Server or Process Server) and you plan to use the same deployment manager profile to manage IBM Business Monitor nodes, augment the profile using the template that IBM Business Monitor provides.
2. Create a custom profile for each node that you plan to add to the server cluster. Alternatively, augment an existing custom profile for each node that you plan to add.

   **Note:** If the database server contains multiple versions of DB2 installed, or multiple DB2 instances, the server's default DB2 version or instance is used for profile creation. To control which DB2 version or instance is used, use the "Installing databases manually" procedure so that the database administrator can ensure that the proper version or instance is used.

To create a profile manually, complete the following steps:

1. Open a command prompt, and navigate to the following directory:

   **app_server_root/bin**

2. Run the **manageprofiles.bat** or **manageprofiles.sh** command using the required parameters. See the reference pages for details of the parameters for each type of profile.

# Chapter 7. Verifying the installation

After you have installed IBM Business Monitor and created a profile, you can optionally use the First Steps Console to verify that the product was installed correctly.

1. Access First Steps.
   - Linux UNIX Open a command window. Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
   - Windows From the Profile Creation Complete panel panel, select the **Launch the IBM Business Monitor first steps** option.
   - Windows Go to **Start** > **All Programs** > **IBM** > **Business Monitor 7.5** > **Profiles** > *profile_name* > **First Steps**.
   - Windows Go to **profile_root\firststeps.wbm** and run the **firststeps.bat** command.

     **Important:** To install or run First Steps on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges by right-clicking **firststeps.bat** and selecting **Run as administrator**. This is required for both administrative and nonadministrative users.
2. From the First Steps console, select the option to perform an installation verification test.
3. Review results.

If you enabled security for IBM Business Monitor, after the installation completes, you must set up users by supplying a user ID and password for the MonitorBusAuth authentication alias. See Specifying credentials in an IBM Business Monitor secured environment for more details.

In addition to the installation verification test, the First Steps console provides options to run the Profile Management Tool, open the WebSphere Application Server administrative console, and open Business Space.

Linux UNIX On a Linux or UNIX system, you might have to change the ownership from root user to a different user. You perform this task on IBM Business Monitor exactly as you would on WebSphere Application Server or Process Server. See the related links below for more information.

If you are creating a new IBM Business Monitor profile or augmenting an existing profile with IBM Business Monitor resulted in a result code of **INSTCONFPARTIALSUCCESS** or **INSTCONFFAILED**, consult the table in the related reference link.

© Copyright IBM Corp. 2005, 2012

# Chapter 8. Determining port numbers

To determine the port number to use with web interfaces such as Business Space and the portlet-based dashboards, review the configuration in the WebSphere Application Server administrative console.

In a network deployment (ND) environment, you normally use a proxy server or an HTTP server for security reasons and for workload balancing. Instead of incoming HTTP requests going directly to a specific cluster member, they go to a proxy server that can spread the requests across the multiple cluster members that perform the work. In this case, you need the host name and port number of the proxy server or web server, which in turn forwards the request to a cluster member.

- To determine the port numbers for an application server, complete the following steps:
  1. In the WebSphere Application Server administrative console, select **Servers** > **Server Types** > **WebSphere application servers**.
  2. Select the name of your server or cluster member (such as **server1**).
  3. Under Communications, click **Ports**.

  The port number to use with web interfaces such as Business Space and the portlet-based dashboards is listed as **WC_defaulthost_secure** in an environment with security and **WC_defaulthost** in an environment without security. This page also provides the port number for the bootstrap port, the SOAP connector port, and other ports that you might be asked to enter while working with IBM Business Monitor.
- To determine the port numbers for a proxy server, complete the following steps:
  1. In the WebSphere Application Server administrative console, select **Servers** > **Server Types** > **WebSphere proxy servers**.
  2. Select the name of your server (such as **proxy**).
  3. Under Communications, click **Ports**.

  The port number to use with web interfaces such as Business Space and the portlet-based dashboards is listed as **PROXY_HTTPS_ADDRESS** in an environment with security and **PROXY_HTTP_ADDRESS** in an environment without security. This page also provides the port number for the bootstrap port, the SOAP connector port, and other ports that you might be asked to enter while working with IBM Business Monitor.

Web modules are deployed to a virtual host (by default named **defaulthost**). Virtual hosts are configured in the administrative console by clicking **Environment** > **Virtual hosts**. The virtual host that you choose for each web module must include the HTTP or HTTPS port that is used by the server (or cluster member) where the web modules are deployed. Additionally, each of the IBM Business Monitor web modules should use the same virtual host. There are web modules in most of the IBM Business Monitor, Business Space, and REST applications (EAR files).

© Copyright IBM Corp. 2005, 2012

# Chapter 9. Configuring the environment

After you have installed IBM Business Monitor in a network deployment (ND) topology, you must complete additional configuration tasks to install required resources and fully prepare your environment for monitoring.

When you create a stand-alone profile for IBM Business Monitor, the required resources are created automatically as part of the profile creation process. You can use the administrative console to check status, or to redeploy a component that has been manually removed, but typically the configuration tasks in this section are required only for network deployment (ND).

## Creating the deployment environment using a pattern

You can use the deployment environment configuration wizard to create the cluster or clusters and configure all the required components for the IBM Business Monitor network deployment (ND) topology.

Before creating clusters and configuring the IBM Business Monitor components, ensure that you have performed the following tasks:

- You have installed IBM Business Monitor.
- You have created the IBM Business Monitor deployment manager profile or augmented an existing deployment manager profile with IBM Business Monitor.
- You have created the MONITOR database.
- You have started the deployment manager.
- You have created and federated at least one IBM Business Monitor custom profile or augmented an existing custom profile with IBM Business Monitor.
- You have started the custom profile or profiles.

Before starting the configuration process, make sure that you are synchronizing node changes automatically (in the administrative console, click **System Administration** > **Console Preferences** and select **Synchronize changes with Nodes**). Otherwise, you must synchronize changes manually after each major step.

Two patterns are available for IBM Business Monitor: the Single Cluster pattern and the Remote Messaging, Remote Support, and web (four-cluster) pattern.

One of the optional steps in the deployment environment configuration wizard includes importing a database design document. The database design document defines the database configuration for the selected deployment environment features and the information from the design document is reflected on the Database page of the wizard. IBM Business Monitor includes a response-driven database design tool (DbDesignGenerator) that prompts users for information on the databases that will be used by IBM Business Monitor (information such as the database platform and the database, schema, and user names). The output of the database design tool is a database design document that is used by the database design tool to create the database scripts.

To configure the deployment environment, complete the following steps:

1. In the administrative console, click **Servers** > **Deployment Environments**.
2. To launch the deployment environment configuration wizard, click **New** on the Deployment Environments page.
   a. The **Create a deployment environment based on a pattern** option is selected.

© Copyright IBM Corp. 2005, 2012

b. Enter a unique name for the deployment environment in the **Deployment environment name** field.

c. If you want to view all of the configuration steps in the wizard, select **Detailed: Show all steps**. If you choose **Fast path: Show only needed steps**, the wizard displays only those pages that do not have assigned default values. Choose **Fast path: Show only needed steps** only if you are agreeable to accepting the system-provided default values for the deployment environment configuration. This topic assumes that you have chosen **Detailed: Show all steps**.

d. Click **Next** to display the Deployment Environment Features page.

3. On the Deployment Environment Features page, select the feature for the deployment environment and click **Next** to either view a list of compatible features, or to view a list of deployment environment patterns. Features represent the runtime processing capabilities of your deployment environment. The list of available features on the Deployment Environment Features page is based on the deployment manager profile. If your deployment manager profile has been augmented to include other products as well as IBM Business Monitor (for example, IBM Business Process Manager) the Deployment Environment Features page lists these features as well. The default value for the deployment environment feature matches the runtime capabilities of your deployment manager.
4. On the Select compatible deployment environment features page, select additional features as necessary and click **Next** to view the list of patterns associated with your feature selections. Only one deployment environment configuration can exist with the **WBM** feature. If a deployment environment configuration with the **WBM** feature already exists, you will not be able to continue, even if the deployment environment configuration has not been generated.
5. On the Select the deployment environment pattern page, select the pattern and click **Next** to display the Select Nodes page.

   The list of patterns that display on the Deployment Environment Patterns page is dynamic. This list is activated by, and dependent on, the following environment conditions and configuration decisions:

   - The platform on which you have installed the software
   - The selections that you have made on the Select the deployment environment feature page and the Select compatible deployment environment features page.

   Typically you will have a choice between the Single Cluster pattern and the Remote Messaging, Remote Support, and Web (four-cluster) pattern. For descriptions of these patterns, see the "High availability (network deployment) topology" page in the planning section.
6. On the Select Nodes page, select the nodes that you want to include in this deployment environment, then click **Next** to display the Cluster members page.

   Select one or more IBM Business Monitor nodes for the deployment environment. You can identify the IBM Business Monitor nodes by an entry for **WBM** in the version column of the list. If a node does not have an entry for **WBM** in the version column and you want to enable it for IBM Business Monitor, augment the node's profile with IBM Business Monitor and restart the deployment environment configuration wizard.

   All selected nodes must be IBM Business Monitor nodes. If you selected additional features in step 3, select nodes that also support the additional features.

   For high-availability and failover environments, select at least two nodes on at least two separate hosts. For additional scalability, select more than two nodes.

   To include a node, select the check box next to the node name.
7. On the Clusters page, assign at least one cluster member on at least one node for each function of the deployment environment.

   By default one cluster member is assigned on each node for each function. You change the number by replacing the number in each column. For network deployment, clusters can collaborate to provide specific functionality to the environment. Depending on your requirements, you assign specific functions to each cluster within the deployment environment, to provide performance, failover, and capacity.

A 0 (zero) value for a node means that the node does not contribute to the selected function, based on features that you have selected.

There must be at least one cluster member assigned for each function. For high-availability and failover environments, indicate at least two cluster members per function. For additional scalability, indicate more cluster members for a function.

After assigning cluster members, you can click **Next** to display the Cluster naming pages for each cluster type of the deployment environment. The Cluster naming substeps that display will vary depending on the deployment environment pattern selected. If you do not want to customize cluster names or cluster member names, use the wizard navigation pane to go directly to the REST services page and continue to the next step.

a. Optional: Customize the cluster names and cluster member names. Use the Cluster naming page to customize cluster names or cluster member names for the cluster type. You can also modify cluster short names and cluster member short names. There is one substep page for each cluster type in the pattern that you have selected. The information on each substep page is as follows:

| Field | Description | Value |
|---|---|---|
| Cluster | A read-only field specifying the functional role of the cluster. | The value varies depending on the cluster type, as follows:<br>• Application Deployment Target<br>• Supporting Infrastructure<br>• Messaging Infrastructure<br>• Web Application Infrastructure<br>For information on the functional role provided by each cluster type, see "Topologies and deployment environment patterns." |
| Cluster name | The system-generated default value for the cluster name. | The default values are based on a naming convention of ***Deployment Environment Name.Cluster type name***, where ***Cluster type name*** is one of the following values:<br>• **AppTarget** - For clusters performing the role of application deployment target<br>• **Messaging** - For clusters performing the role of messaging infrastructure<br>• **Support** - For clusters performing the role of supporting infrastructure<br>• **Web** - For clusters performing the role of supporting web applications |
| Cluster member name | The system-generated default value for the cluster member name. Servers that are a part of a cluster are called cluster members. | Accept the system-generated default value or specify a name of your choosing. The default value for the cluster member name is based on the following naming convention: ***cluster name.node name.node number sequence***. The number of cluster member names that display in the table match the number of cluster members that you entered for the cluster type column and node row on the Clusters page. |

8. On the System REST Service endpoints page, configure service endpoints for Representational State Transfer (REST) application programming interfaces (APIs).

   If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. For the host name and port, if you want REST requests to go directly to the application server, enter the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, enter the host name and port of the proxy server or HTTP server. In the second case, you must have already set up a proxy server or an HTTP server. Otherwise, skip this page and configure the endpoints later.

   a. Configure a full URL path for all REST services by selecting either **https://** or **http://** from the **Protocol** list.
   b. Enter the name of the proxy server or HTTP server in the **Host Name or Virtual Host in a Load-Balanced Environment** field.

      Enter the host or virtual host name and port number that a client needs to communicate with the server or cluster. In a clustered environment, this is typically the load balancer host name and port. If you leave the host and port fields empty, the values default to the values of an individual cluster member host and its HTTP port. For a load-balanced environment, you must later change the default values to the virtual host name and port of your load balancer. Make sure to designate a fully qualified host name.
   c. In the **Port** field, enter the port that a client needs to communicate with the server or cluster.
   d. In the table of REST services, if you want to modify the description of the REST service endpoint, overtype the entry in the Description field. The other fields are read-only.
   e. Click **Next** to go to the Import the database configuration page.

9. Optional: On the Import the database configuration page, click **Browse** to go to the database design document or enter the path to the database design document and then click **Next** to go to the Data sources page. If you import a design document, the information from the design document is reflected on the Database page of the wizard. The design document can be based on a database design that you created using the database design tool, or it can be the supplied design document based on the pattern and feature that you have selected.
10. On the Database page, configure the database parameters for data sources of the deployment environment, then click **Next** to go to the Security page.

    On this page, define the database information for the components that are included in this deployment environment. Where possible, the wizard supplies default information for the parameters, but change those values to match the values that you defined when you planned the environment. If you change providers, you can click the **Edit Provider** button to edit the provider that you selected.

    **Note:** If you imported a database design document, the information on the Database page reflects the data source configuration as it exists in the database design document that you imported. If you make changes to the data source configuration after importing a database design document, your changes might be incompatible with the DDL generated by the database design tool and the original values.

    Whether or not this step displays for a fast path deployment environment configuration is conditional. This step displays for a fast path deployment environment configuration if more than one database has been defined.

    This step always displays if you are using a DB2 for z/OS or an Oracle database provider.

    The IBM Business Monitor feature provides the following entries:

| Component | Data source |
|---|---|
| Business Monitor messaging engine data source | Data source for the IBM Business Monitor messaging engine. |

| Component | Data source |
| --- | --- |
| Cognos Content Store | Data source for the IBM Cognos Business Intelligence content store. (Displayed only if IBM Cognos BI has been installed and not yet configured.)<br><br>The Content Store data source is created in the IBM Cognos BI configuration and not as a WebSphere data source. Leave the **Create tables** option checked; otherwise this data source is marked as a deferred configuration. IBM Cognos BI creates the tables on first startup.<br><br>A WebSphere authentication alias (Cognos_JDBC_Alias) is created based on the user name and password provided for this data source. This authentication alias is not used directly by IBM Cognos BI but it enables all database user names and passwords to be maintained using the same process. On server startup, IBM Business Monitor sends the current user name and password values to the IBM Cognos BI configuration.<br><br>For DB2 on z/OS, you must install the COGNOSCS database manually. |
| Business Space | Data source for the Business Space component. If you select the **Create tables** option, the schema name used by Business Space must already exist in the database.<br>**Important:** For Oracle only, you must run app_server_root/`dbscripts/BusinessSpace/Oracle/createSchema_BusinessSpace.sql` to create the schema user and grant the required rights. |

If you selected other product features for this topology, other feature-specific entries might also appear here.

The default schema names that are displayed on this page might conflict with your site naming convention or might conflict with existing schemas. As such, it is likely that you will need to change the schema name.

**Note:** For DB2 for z/OS databases, the schema name that is configured on the panel will be used for the DB2 z/OS SQLID value. If the DB2 z/OS SQLID value needs to be different in your environment, then after the deployment environment wizard is finished, you can manually update the data sources that have been created and change the currentSQLID Custom Property to the correct value.

You can edit all key parameters, such as the database name, whether or not to create tables, the data source runtime user name, and the user name and password for the data source to connect to the database.

**Note:** For DB2 for z/OS databases, the database name is the database subsystem name. For other versions of DB2, the database name is the MONITOR database name. For Oracle databases, the database name is the Oracle System ID.

You can select which database to use for the given component.

The **Create tables** option is not available if you are using a DB2 for z/OS or an Oracle database provider.

For Oracle, the **Schema** field is disabled and empty, and the **User name** is not pre-filled with the common database user name. You must enter a user name and password for each data source.

**Note:** No validation takes place to ensure that user names are unique, so be aware that you might create a duplicate user name, resulting in table conflicts.

11. On the Security page, enter the user IDs and passwords that are needed to configure the IBM Business Monitor components. The IBM Business Monitor feature provides the following entries:

| Component | ID and Password |
| --- | --- |
| Authentication alias for the CEI event service JMS resources | Specify the user ID and password to use to secure the default common event infrastructure (CEI) service integration bus. |
| Cognos Administration access authentication | Specify a user ID and password with administrative rights to the IBM Cognos BI service. (Displayed only if IBM Cognos BI has been installed and not yet configured.) |

If you selected other product features for this topology, other feature-specific entries might also appear here.

12. Optional: If the Business Process Choreographer page is displayed, set parameters for the Business Process Choreographer configuration and then click **Next** to display the Web application context roots page. On this page you specify the values for:
    - Security roles
    - Authentication aliases
13. Optional: If the Web application context roots page is displayed, set the context root for component-based web applications in your deployment environment or accept the system-provided default values for the context roots. Then click **Next** to display the Summary page.

    The table contains the following control information.

    **Web Application**
    The name of the web application.

    Some of the components that are part of the deployment environment you are creating contain web applications. The **Web application** column can include the following components:
    - Business Process Choreographer Explorer
    - Business Space
    - Business Process Rules Manager

    **Context Root**
    The current value of the context root for the component.

    By default, the default context root for the web application applies. You can change the context roots by typing over the value in the **Context Root** field.

    **Note:** The Business Space context root is read only and cannot be edited.
14. Verify that the information on the Summary page is correct and click **Finish and Generate Environment** to save and complete the configuration of the deployment environment. To exit without completing the configuration, click **Finish**.

    Clicking **Finish** saves the deployment environment configuration - but does not generate it.

    Click **Cancel** cancels the deployment configuration and does not save the configuration.
15. If you clicked **Finish and Generate Environment** to generate a deployment environment, stop and restart all clusters, nodes, and the deployment manager.

If you selected not to generate the environment at the end of the deployment environment configuration wizard (by clicking **Finish** rather than **Finish and Generate Environment**), you can view the deployment environment configuration at **Server** > **Deployment Environments** > *name of deployment environment*. From there, you can click **Generate** to generate the environment. When the configuration completes, you can examine the configuration files to view the changes.

Either save the changes to the master configuration or discard them. If you click a deployment environment in the list, and there are still configuration steps to perform, you will see a list of deferred configuration steps. After generating a deployment environment, stop and restart all clusters, nodes, and the deployment manager.

**Important:** The cluster that will be running the IBM Cognos BI service requires that each cluster member be started individually. You must wait for the IBM Cognos BI service to initialize fully before starting the next cluster member.

## Importing deployment environment definitions based on design documents

You can import an existing deployment environment definition based on a design document from another deployment manager to use as a base for configuring a new deployment environment.

- You must have a copy of an exported deployment environment design document from another deployment manager.
- You must be able to access the deployment environment design document (an XML file) from the deployment manager into which you are importing the deployment environment design.
- The deployment manager that imports the deployment environment definition must support at least all of the functions that are defined in the deployment environment design document. For example, you can import a deployment environment design that was created on a WebSphere Enterprise Service Bus deployment manager into a Process Server deployment manager but not vice versa.

**Note:** When security and role-based authorization are enabled, you must log in to the administrative console as an administrator to perform this task.

**Important:** You cannot import multiple deployment environment design documents from a compressed file at the same time. You must extract the design documents from the compressed file and then import the XML files one at a time.

Before starting the configuration process, make sure that you are synchronizing node changes automatically (in the administrative console, click **System Administration** > **Console Preferences** and select **Synchronize changes with Nodes**). Otherwise, you must synchronize changes manually after each major step.

Importing an existing deployment environment design to create a new one can minimize the amount of time you spend configuring a deployment environment. If an existing environment is similar to the one you want to create, export it and then import it into the deployment manager that you are configuring.

1. In the administrative console, click **Servers** > **Deployment Environments**.
2. Click **Import** in the Deployment Environments page to launch the Deployment Environment Configuration wizard.

   The wizard starts with **Create a deployment environment based on an imported design** selected.
3. Click **Browse** and select the deployment environment design document (XML file) to import or type the full path to it.
4. Click **Next** to load the configuration and launch the Import deployment environment wizard.

   The wizard displays the Select Nodes page, unless all the node names match currently federated notes. If all nodes match, the wizard displays the Database page.

   **Important:** Clicking configure in any panel in the wizard configures the deployment environment with the current values.
5. Optional: From the list of possible nodes on the Select Nodes page, select the nodes to include in the deployment environment and click **Next**.

   To include a node, select the check box next to the node name.

   **Important:** **Next** is not available if the nodes selected do not meet the constraints imposed by the imported deployment environment design. For example, if there is a requirement for the deployment environment to contain a node named “Mandatory_Node” and 3 other nodes with any name, you will be unable to continue until you select “Mandatory_Node” and 3 other nodes.

6. On the Clusters page, assign at least one cluster member on at least one node for each function of the deployment environment.

   By default one cluster member is assigned on each node for each function. You change the number by replacing the number in each column. For network deployment, clusters can collaborate to provide specific functionality to the environment. Depending on your requirements, you assign specific functions to each cluster within the deployment environment, to provide performance, failover, and capacity.

   A 0 (zero) value for a node means that the node does not contribute to the selected function, based on features that you have selected.

   There must be at least one cluster member assigned for each function. For high-availability and failover environments, indicate at least two cluster members per function. For additional scalability, indicate more cluster members for a function.

   After assigning cluster members, you can click **Next** to display the Cluster naming pages for each cluster type of the deployment environment. The Cluster naming substeps that display will vary depending on the deployment environment pattern selected. If you do not want to customize cluster names or cluster member names, use the wizard navigation pane to go directly to the REST services page and continue to the next step.

   a. Optional: Customize the cluster names and cluster member names. Use the Cluster naming page to customize cluster names or cluster member names for the cluster type. You can also modify cluster short names and cluster member short names. There is one substep page for each cluster type in the pattern that you have selected. The information on each substep page is as follows:

| Field | Description | Value |
|---|---|---|
| Cluster | A read-only field specifying the functional role of the cluster. | The value varies depending on the cluster type, as follows:<br>• Application Deployment Target<br>• Supporting Infrastructure<br>• Messaging Infrastructure<br>• Web Application Infrastructure<br>For information on the functional role provided by each cluster type, see "Topologies and deployment environment patterns." |
| Cluster name | The system-generated default value for the cluster name. | The default values are based on a naming convention of ***Deployment Environment Name.Cluster type name***, where ***Cluster type name*** is one of the following values:<br>• **AppTarget** - For clusters performing the role of application deployment target<br>• **Messaging** - For clusters performing the role of messaging infrastructure<br>• **Support** - For clusters performing the role of supporting infrastructure<br>• **Web** - For clusters performing the role of supporting web applications |

| Field | Description | Value |
| --- | --- | --- |
| Cluster member name | The system-generated default value for the cluster member name. Servers that are a part of a cluster are called cluster members. | Accept the system-generated default value or specify a name of your choosing. The default value for the cluster member name is based on the following naming convention: ***cluster name.node name.node number sequence***. The number of cluster member names that display in the table match the number of cluster members that you entered for the cluster type column and node row on the Clusters page. |

7. On the System REST Service endpoints page, configure service endpoints for Representational State Transfer (REST) application programming interfaces (APIs).

   If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. For the host name and port, if you want REST requests to go directly to the application server, enter the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, enter the host name and port of the proxy server or HTTP server. In the second case, you must have already set up a proxy server or an HTTP server. Otherwise, skip this page and configure the endpoints later.

   a. Configure a full URL path for all REST services by selecting either **https://** or **http://** from the **Protocol** list.

   b. Enter the name of the proxy server or HTTP server in the **Host Name or Virtual Host in a Load-Balanced Environment** field.

      Enter the host or virtual host name and port number that a client needs to communicate with the server or cluster. In a clustered environment, this is typically the load balancer host name and port. If you leave the host and port fields empty, the values default to the values of an individual cluster member host and its HTTP port. For a load-balanced environment, you must later change the default values to the virtual host name and port of your load balancer. Make sure to designate a fully qualified host name.

   c. In the **Port** field, enter the port that a client needs to communicate with the server or cluster.

   d. In the table of REST services, if you want to modify the description of the REST service endpoint, overtype the entry in the Description field. The other fields are read-only.

   e. Click **Next** to go to the Import the database configuration page.

8. Optional: On the Import the database configuration page, click **Browse** to go to the database design document or enter the path to the database design document and then click **Next** to go to the Data sources page. If you import a design document, the information from the design document is reflected on the Database page of the wizard. The design document can be based on a database design that you created using the database design tool, or it can be the supplied design document based on the pattern and feature that you have selected.

9. On the Database page, configure the database parameters for data sources of the deployment environment, then click **Next** to go to the Security page.

   On this page, define the database information for the components that are included in this deployment environment. Where possible, the wizard supplies default information for the parameters, but change those values to match the values that you defined when you planned the environment. If you change providers, you can click the **Edit Provider** button to edit the provider that you selected.

   **Note:** If you imported a database design document, the information on the Database page reflects the data source configuration as it exists in the database design document that you imported. If you

make changes to the data source configuration after importing a database design document, your changes might be incompatible with the DDL generated by the database design tool and the original values.

Whether or not this step displays for a fast path deployment environment configuration is conditional. This step displays for a fast path deployment environment configuration if more than one database has been defined.

This step always displays if you are using a DB2 for z/OS or an Oracle database provider.

The IBM Business Monitor feature provides the following entries:

| Component | Data source |
|---|---|
| Business Monitor messaging engine data source | Data source for the IBM Business Monitor messaging engine. |
| Cognos Content Store | Data source for the IBM Cognos Business Intelligence content store. (Displayed only if IBM Cognos BI has been installed and not yet configured.)<br><br>The Content Store data source is created in the IBM Cognos BI configuration and not as a WebSphere data source. Leave the **Create tables** option checked; otherwise this data source is marked as a deferred configuration. IBM Cognos BI creates the tables on first startup.<br><br>A WebSphere authentication alias (Cognos_JDBC_Alias) is created based on the user name and password provided for this data source. This authentication alias is not used directly by IBM Cognos BI but it enables all database user names and passwords to be maintained using the same process. On server startup, IBM Business Monitor sends the current user name and password values to the IBM Cognos BI configuration.<br><br>For DB2 on z/OS, you must install the COGNOSCS database manually. |
| Business Space | Data source for the Business Space component. If you select the **Create tables** option, the schema name used by Business Space must already exist in the database.<br>**Important:** For Oracle only, you must run app_server_root/`dbscripts/BusinessSpace/Oracle/createSchema_BusinessSpace.sql` to create the schema user and grant the required rights. |

If you selected other product features for this topology, other feature-specific entries might also appear here.

The default schema names that are displayed on this page might conflict with your site naming convention or might conflict with existing schemas. As such, it is likely that you will need to change the schema name.

**Note:** For DB2 for z/OS databases, the schema name that is configured on the panel will be used for the DB2 z/OS SQLID value. If the DB2 z/OS SQLID value needs to be different in your environment, then after the deployment environment wizard is finished, you can manually update the data sources that have been created and change the currentSQLID Custom Property to the correct value.

You can edit all key parameters, such as the database name, whether or not to create tables, the data source runtime user name, and the user name and password for the data source to connect to the database.

**Note:** For DB2 for z/OS databases, the database name is the database subsystem name. For other versions of DB2, the database name is the MONITOR database name. For Oracle databases, the database name is the Oracle System ID.

You can select which database to use for the given component.

The **Create tables** option is not available if you are using a DB2 for z/OS or an Oracle database provider.

For Oracle, the **Schema** field is disabled and empty, and the **User name** is not pre-filled with the common database user name. You must enter a user name and password for each data source.

**Note:** No validation takes place to ensure that user names are unique, so be aware that you might create a duplicate user name, resulting in table conflicts.

10. On the Security page, enter the user IDs and passwords that are needed to configure the IBM Business Monitor components. The IBM Business Monitor feature provides the following entries:

| Component | ID and Password |
|---|---|
| Authentication alias for the CEI event service JMS resources | Specify the user ID and password to use to secure the default common event infrastructure (CEI) service integration bus. |
| Cognos Administration access authentication | Specify a user ID and password with administrative rights to the IBM Cognos BI service. (Displayed only if IBM Cognos BI has been installed and not yet configured.) |

If you selected other product features for this topology, other feature-specific entries might also appear here.

11. Optional: If the Business Process Choreographer page is displayed, set parameters for the Business Process Choreographer configuration and then click **Next** to display the Web application context roots page. On this page you specify the values for:
    - Security roles
    - Authentication aliases
12. Optional: If the Web application context roots page is displayed, set the context root for component-based web applications in your deployment environment or accept the system-provided default values for the context roots. Then click **Next** to display the Summary page.

    The table contains the following control information.

    **Web Application**
    The name of the web application.

    Some of the components that are part of the deployment environment you are creating contain web applications. The **Web application** column can include the following components:
    - Business Process Choreographer Explorer
    - Business Space
    - Business Process Rules Manager

    **Context Root**
    The current value of the context root for the component.

    By default, the default context root for the web application applies. You can change the context roots by typing over the value in the **Context Root** field.

    **Note:** The Business Space context root is read only and cannot be edited.
13. Verify that the information on the Summary page is correct and click **Finish and Generate Environment** to save and complete the configuration of the deployment environment. To exit without completing the configuration, click **Finish**.

    Clicking **Finish** saves the deployment environment configuration - but does not generate it.

    Click **Cancel** cancels the deployment configuration and does not save the configuration.
14. If you clicked **Finish and Generate Environment** to generate a deployment environment, stop and restart all clusters, nodes, and the deployment manager.

If you selected not to generate the environment at the end of the deployment environment configuration wizard (by clicking **Finish** rather than **Finish and Generate Environment**), you can view the deployment

environment configuration at **Server** > **Deployment Environments** > *name of deployment environment*. From there, you can click **Generate** to generate the environment. When the configuration completes, you can examine the configuration files to view the changes.

Either save the changes to the master configuration or discard them. If you click a deployment environment in the list, and there are still configuration steps to perform, you will see a list of deferred configuration steps. After generating a deployment environment, stop and restart all clusters, nodes, and the deployment manager.

**Important:** The cluster that will be running the IBM Cognos BI service requires that each cluster member be started individually. You must wait for the IBM Cognos BI service to initialize fully before starting the next cluster member.

## Adding an IBM Business Monitor deployment environment to an IBM Business Process Manager server deployment environment

To add an IBM Business Monitor deployment environment on top of an existing IBM Business Process Manager deployment environment using the deployment environment configuration wizard, there are some additional steps to perform.

You must either install and register the IBM BPM widgets into the IBM Business Monitor Business Space (the easiest and therefore preferred method) or install and register the IBM Business Monitor widgets into the IBM BPM Business Space.

Create the IBM Business Monitor deployment environment following the steps in the "Creating the deployment environment using a pattern" parent topic.

Next, either install the IBM BPM widgets into the IBM Business Monitor Business Space or install the IBM Business Monitor widgets into the IBM BPM Business Space. The first is the easiest and therefore the preferred method.

### Installing IBM Business Process Manager widgets into IBM Business Monitor Business Space

To install IBM Business Process Manager widgets into IBM Business Monitor Business Space, install the widgets and then register the Representational State Transfer (REST) service endpoints to the widgets.

After you have generated the deployment environment, complete the following steps:

1. Install the IBM BPM Business Space widgets into the IBM Business Monitor deployment environment. The Business Space widgets are located under the IBM BPM root directory (such as `IBM/BPM`) `/BusinessSpace/registryData/`*`product_name`*`/widgets`. To install IBM BPM-only widgets, specify *`BPM_install_root`*`/BusinessSpace/registryData/BPM/widgets` as the value for the **-widgets** parameter. For example:

   ```
   AdminTask.installBusinessSpaceWidgets('[-clusterName cluster_name -widgets
    install_root/BusinessSpace/registryData/BPM/widgets/]')
   ```

2. Register the REST service endpoints to the widgets. The REST services are only available on the IBM BPM clusters and they must be registered in the IBM Business Monitor cluster so that the widgets can be used from the IBM Business Monitor Business Space.

   You can register the REST service endpoints either in the administrative console or from the command line. Follow the instructions in the "Configuring Business Space and registering REST endpoints on the administrative console" or "Registering Business Space widget REST service endpoints using the command line" related tasks.

   - For the **-clusterName** parameter, specify the IBM BPM cluster name where the REST services are installed.
   - For the **-businessSpaceClusterName** parameter, specify the cluster where IBM Business Monitor Business Space is installed.

The following examples use Jython.

- For a single-cluster environment:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName <WPS cluster name> -type "{com.ibm.bpm}BFM" -businessSpaceClus
```

- For a four-cluster environment, where IBM Business Monitor Business Space is installed on the web cluster of the deployment environment:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName WPSCluster.AppTarget -type "{com.ibm.bpm}BFM" -businessSpaceC
```

### Installing IBM Business Monitor widgets into BPM Business Space

To install IBM Business Monitor widgets into IBM Business Process Manager Business Space, install the widgets, register the Representational State Transfer (REST) service endpoints to the widgets, and complete the IBM Cognos Business Intelligence widgets endpoint configuration.

After you have generated the deployment environment, complete the following steps:

1. Install the IBM Business Monitor Business Space widgets into the IBM BPM deployment environment.

   ```
   AdminTask.installBusinessSpaceWidgets('[-clusterName cluster_name -widgets
    install_root/BusinessSpace/registryData/WBM/widgets/]')
   ```

2. Register the REST service endpoints to the widgets. The REST services are only available on the IBM BPM clusters and they must be registered in the IBM Business Monitor cluster so that the widgets can be used from the IBM Business Monitor Business Space.

   You can register the REST service endpoints either in the administrative console or from the command line. Follow the instructions in the "Configuring Business Space and registering REST endpoints on the administrative console" or "Registering Business Space widget REST service endpoints using the command line" related tasks.

   - For the **-clusterName** parameter, specify the IBM BPM cluster name where the REST services are installed.
   - For the **-businessSpaceClusterName** parameter, specify the cluster where IBM Business Monitor Business Space is installed.

   The following examples use Jython.

   - For a single-cluster environment:

     ```
     AdminTask.registerRESTServiceEndpoint('[-clusterName <WPS cluster name> -type "{com.ibm.bpm}BFM" -businessSpaceClus
     ```

   - For a four-cluster environment, where IBM Business Monitor Business Space is installed on the web cluster of the deployment environment:

     ```
     AdminTask.registerRESTServiceEndpoint('[-clusterName WPSCluster.AppTarget -type "{com.ibm.bpm}BFM" -businessSpaceC
     ```

3. Complete the IBM Cognos BI widgets service endpoint configuration by following the instructions in "Configuring IBM Business Monitor and Business Space to use an existing IBM Cognos BI service."

## Creating the deployment environment using custom topology

Instead of using one of the provided deployment environment patterns, you can set up your own clusters and configure the IBM Business Monitor components in a network deployment (ND) topology.

Before creating clusters and configuring the IBM Business Monitor components, ensure that you have performed the following tasks:

- You have installed IBM Business Monitor.
- You have created the IBM Business Monitor deployment manager profile or augmented an existing deployment manager profile with IBM Business Monitor.
- You have created the MONITOR database.
- You have started the deployment manager.
- You have created and federated at least one IBM Business Monitor custom profile or augmented an existing custom profile with IBM Business Monitor.
- You have started the custom profile or profiles.

The following instructions describe how to create clusters, configure the common event infrastructure (CEI) event service, and install and configure the required components using the configuration wizard or the wsadmin commands.

## Creating IBM Business Monitor clusters

In a network deployment (ND) environment, IBM Business Monitor components must be deployed to clusters.

Before creating clusters and configuring the IBM Business Monitor components, ensure that you have performed the following tasks:

- You have installed IBM Business Monitor.
- You have created the IBM Business Monitor deployment manager profile or augmented an existing deployment manager profile with IBM Business Monitor.
- You have created the MONITOR database.
- You have started the deployment manager.
- You have created and federated at least one IBM Business Monitor custom profile or augmented an existing custom profile with IBM Business Monitor.
- You have started the custom profile or profiles.

Use an existing custom profile to create the first cluster member. You can add as many additional cluster members as you want in each cluster that you create (see "Adding cluster members"). To create the IBM Business Monitor cluster, complete the following steps from the administrative console:

1. In the navigation panel, click **Servers** > **Clusters** > **WebSphere application server clusters**.
2. Click **New** to start the Create a new cluster wizard.
3. Specify a name for the cluster.
4. Select **Prefer local** to enable host-scoped routing optimization. This setting improves performance by looking up EJBs in a cluster member on the same node whenever possible.
5. Click **Next** to proceed to the Create first cluster member step.
6. Specify the name of the first cluster member.
7. Specify a node for the first cluster member. This node must be an IBM Business Monitor node.
8. Select the option to **Create the member using an application server template**.
9. Select an application server template containing the text ***defaultWBM*** in the name, and click **Next**.

   **Important:** If there is no template with defaultWBM in the name, make sure that you have selected a node that has been augmented with IBM Business Monitor.

   If the first cluster member is not created using an application server template with defaultWBM in the name, your IBM Business Monitor environment will not function properly, and you will have to delete all the existing cluster members and re-create the first cluster member.
10. Click **Next** to proceed to the Create additional cluster members step.
11. Optional: To add additional cluster members, complete the following steps for each cluster member:
    a. Specify a unique name for the additional member. The name must be unique within the node.
    b. Specify a node for the additional cluster member. This node must be an IBM Business Monitor node.
    c. Click **Add member**.
12. Click **Next** to proceed to the summary panel.
13. Review the information and click **Finish**.
14. Click **Save** to save changes to the master configuration.

After initially creating a cluster, you can add additional cluster members at any time.

To start a cluster the first time after the IBM Cognos Business Intelligence service is installed, start each server individually. Do not use the ripplestart option, because this option does not give IBM Cognos BI enough time to initialize.

The administrative console might report issues when you first start the IBM Cognos Business Intelligence server. The initialization of each server instance in the IBM Cognos Business Intelligence content store database and disk area during the first startup takes much longer than a normal IBM Cognos Business Intelligence startup.

## Adding cluster members

You can add as many cluster members as you want to an existing cluster.

**Important:** If the first cluster member is not created using an application server template with defaultWBM in the name, your IBM Business Monitor environment will not function properly, and you will have to delete all the existing cluster members and re-create the first cluster member.

To create additional cluster members, complete the following steps:

1. In the navigation panel, click **Servers** > **Clusters** > **WebSphere application server clusters** > ***cluster_name*** > **Cluster members**.
2. Click **New** to start the Create new cluster members wizard.
3. For each new cluster member, complete the following steps:
   a. Specify a unique name for the additional member. The name must be unique within the node.
   b. Specify a node for the additional cluster member. This node must be an IBM Business Monitor node.
   c. Click **Add member**.
4. Click **Next** to proceed to the summary panel.
5. Review the information and click **Finish**.
6. Click **Save** to save changes to the master configuration.

   **Note:** During the IBM Business Monitor installation, the Cognos service is also installed on the node and will be configured on the new server when a member is added to a cluster.

## Federating additional nodes

After you have created a high availability environment in a network deployment cell, you can federate additional nodes into the cell at a later time if needed.

**Important:** IBM Business Monitor does not support portal-based dashboards in the same cell as IBM Business Monitor server v8.0.

To federate existing nodes into the deployment manager, complete the following steps for each node:

1. Start the deployment manager.
2. From the profile directory corresponding to the node you want to federate, run the **addNode** command, specifying the host name of the deployment manager and optionally, the SOAP connector port number of the deployment manager.

   **profile_root\bin\addNode.bat** *dmgr_host_name* [*dmgr_soap_port*]

   **profile_root/bin/addNode.sh** *dmgr_host_name* [*dmgr_soap_port*]

   To run the command with tracing enabled, use the **-trace** option; for example: **addNode** *host_name* **-trace**

   For additional details on how to run the **addNode** command, see the related information in the WebSphere Application Server information center.

## Configuring CEI event services

Before configuring the IBM Business Monitor components using the administrative console, you must have a Common Event Infrastructure (CEI) event service in your network deployment cell that IBM Business Monitor can use to send events. The same CEI event service can also be used to receive events.

If you created a stand-alone profile for IBM Business Monitor or used the deployment environment configuration wizard, a CEI event service has already been created for you. If you are adding IBM Business Monitor on Process Server topology, you can use the CEI event service that is deployed by Process Server for IBM Business Monitor. Otherwise, follow the instructions on this page to create a new CEI event service.

Use the **wbmDeployCEIEventService** command to install a CEI event service on a server or cluster and create the resources it requires (the service integration bus and messaging engine). You can also configure security and enable the default CEI event service data store if required. (The event service data store is not recommended for production environments.) In the core topology for high availability, the CEI event service is installed on the support cluster.

To install and configure a new CEI event service, complete the following steps:

1. Open a command prompt, and change directories to the **bin** directory of the deployment manager profile (by default, DMGR01) where WebSphere Application Server is installed, or to the **bin** directory of the stand-alone profile in a single-server environment.
2. Launch **wsadmin** by running the following command:
   - **wsadmin.sh**
   - **wsadmin.bat**
3. Run the **wbmDeployCEIEventService** command interactively by entering the following at the command line:

   ```
   (jacl) $AdminTask wbmDeployCEIEventService {-interactive}
   (jython) AdminTask.wbmDeployCEIEventService('-interactive')
   ```

   Alternatively, you can run the command by providing all the parameters. For an example, see "Configuring IBM Business Monitor components using wsadmin commands" in the related links.
4. Save the results using the following command:

   ```
   (jacl) $AdminConfig save
   (jython) AdminConfig.save()
   ```
5. To synchronize the nodes, in the administrative console, click **System administration > Nodes**, select all of the nodes, and click **Full Resynchronize**.
6. Restart the deployment manager to see the CEI links show up in the administrative console.

The CEI event service is enabled.

For a full list of parameters and an example, see IBM Business Monitor CEI event service

If you did not perform the data store step while running **wbmDeployCEIEventService**, you can optionally create the data store for the CEI event service later. See "Configuring a CEI database" for instructions.

## Configuring the environment using the configuration wizard

You can configure the required IBM Business Monitor environment using the configuration wizard in the administrative console.

You must have completed the following tasks:

- Created and federated at least one IBM Business Monitor custom profile or augmented an existing custom profile with IBM Business Monitor (see "Creating and augmenting profiles").

- Created at least one cluster using the **defaultWBM** application server template (see "Creating IBM Business Monitor clusters").
- Configured a local Common Event Infrastructure (CEI) event service that IBM Business Monitor can use to send and receive events (see "Configuring CEI event services").

Before starting the configuration process, make sure that you are synchronizing node changes automatically (in the administrative console, click **System Administration** > **Console Preferences** and select **Synchronize changes with Nodes**). Otherwise, you must synchronize changes manually after each major step.

You can configure the required and optional components using the IBM Business Monitor configuration section of the administrative console. For instructions to manually configure all of the IBM Business Monitor components, use the related information links to access the task information.

1. In the navigation panel, click **Servers** > **IBM Business Monitor configuration**. A list of required and optional components is displayed. Review the status of each component. If you have an ND environment and have not configured a deployment environment, none of the components will be installed or configured, and you must complete the remaining steps to install and configure the components.
2. Configure the outbound CEI event service by completing the following steps. The outbound CEI event service is used to send events from IBM Business Monitor, including alerts. You must configure an event emitter factory to point to the outbound CEI event service.

   **Important:** Before configuring the event emitter factory, you must have a local CEI service that IBM Business Monitor can use to send events. If you need to create a local CEI service, see “Configuring CEI event services” on page 110 for instructions.

   a. In the list of components, click **Outbound CEI event service**. The status for the outbound CEI event service and event emitter factory is displayed. If you have an existing MonitorEmitterFactory, the name of the CEI event service that the emitter factory is configured to use is listed in the status box. If you have not already configured the emitter factory, you will see the message "Local CEI event service exists, but event emitter factory does not exist." In that case, you must create and configure the emitter factory.
   b. Under **Configure an event emitter factory**, select the server or cluster for the event emitter factory. All available servers and clusters are listed. You can select only servers that have a CEI event service configured. (The available servers and clusters are shown with asterisks (*)). If you have more than one server with the same name, be sure to choose the server on the correct node.
   c. To launch the configuration wizard, click **Configure the Event Emitter Factory**. An outbound event emitter factory named MonitorEmitterFactory is created for the cell. The status box for the outbound CEI event service is updated to indicate the CEI event service that the MonitorEmitterFactory is configured to use.
   d. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.
3. Create the service integration bus and configure the messaging engine by completing the following steps. IBM Business Monitor requires its own bus and messaging engine before it can monitor events.

   If you do not have an existing bus, one is created for you when you configure the messaging engine. The bus is named **MONITOR.<*cell_name*>.Bus** and the name cannot be changed.

   a. In the list of components, click **Messaging engine**. The status for the service integration bus and the messaging engine is displayed.
   b. To launch the configuration wizard, click **Configure the Messaging Engine**.
   c. On the **Select a bus member** panel, choose one of the following options to select the location where the messaging engine will be created, and click **Next**:
      - **Cluster**: Choose this option to create the messaging engine on an existing cluster. You must select the cluster name from the list.

- **Server**: Choose this option to create the messaging engine on a server. You must select the server from the list. If you have more than one server with the same name, be sure to choose the server on the correct node.

d. On the **Select the type of message store** panel, choose one of the following options, and click **Next**:
   - **Data store**: A data store is a message store that contains a set of tables that are accessible to all members of the cluster that hosts the messaging engine.
   - **File store**: A file store is a message store that uses files in a file system through the operating system. This option is not available if you chose **Cluster** on the **Select a bus member** panel.

e. If you are using a data store, choose one of the following options on the **Provide the message store properties** panel:
   - **Create a default data source with generated JNDI name**: By default, the data store uses Derby. This option is not available if you selected **Cluster** on the **Select a bus member** panel.
   - **Use an existing data source**: If you select this option, complete the following fields:
     - **Data source JNDI name**: Select the JNDI name that corresponds to the database that you are planning to use. For example, **jdbc/wbm/MonitorMEDatabase**.
     - **Schema name**: Enter the schema name. For example, **MONME00**.
     - **Authentication alias**: Select the authentication alias that you are planning to use. You must select the authentication alias if you want the tables to be created. For example, **Monitor_JDBC_Alias**.
     - **Create tables**: Select this option to create the tables in the database. If you do not select this option, the database administrator must create the tables.

f. On the **Confirm** panel, review the information and click **Finish** to complete the configuration. The bus and messaging engine status boxes are updated with the new configuration information.

   **Note:** You might have to wait a few moments for the messaging engine to start successfully.

g. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.

4. Verify that the bus and messaging engine have the correct user ID for your environment:
   a. In the navigation panel, click **Security** > **Bus Security**.
   b. Click the bus for the IBM Business Monitor server. The Buses configuration properties page is displayed.
   c. Under Additional Properties, click **Security**. Another properties page is displayed.
   d. Under Authorization Policy, click **Users and groups in the bus connector role**.
   e. Verify that your user ID exists. If it does not exist, complete these steps to add it:
      1) Click **New**.
      2) Select **Users**, and a enter a filter that will find your user ID. Click **Next**.
      3) Select your ID from the list and click **Next**.
      4) Review the changes and click **Finish**.
   f. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.

5. Install the IBM Business Monitor action services application by completing the following steps. The action services application invokes actions, such as sending dashboard alerts or email notifications, when it receives defined situation events emitted by and other applications. Situation events typically indicate business situations that need attention, such as a printer running out of paper or a metric exceeding a certain value.
   a. In the list of components, click **Action services**. The status for the application is displayed. If the application is properly installed, the location of the installed application is listed in the status box.

b. Under **Deploy action services**, select the server or cluster for the action services application from the list. All available servers and clusters are listed. You must select a server where IBM Business Monitor has been installed. If you have more than one server with the same name, be sure to choose the server on the correct node.

c. To install the application, click **Deploy Action Services**. The application is installed and the Monitor action services group profile is created. The application status box is updated with the location of the installed application, named IBM_WBM_ACTIONSERVICES. If this application has been installed to a cluster, the application will appear unavailable until all nodes in the cluster have been synchronized.

d. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.

6. Install the Monitor scheduled services application by completing the following steps. You must install this application to schedule recurring services, such as the data movement service and the key performance indicator (KPI) history for monitor models.

   a. In the list of components, click **Monitor scheduled services**. The status for the application is displayed. If the application is properly installed, the location of the installed application is listed in the status box.

   b. Under **Deploy Monitor Scheduled Services**, select the server or cluster for the Monitor scheduled services application from the list. All available servers and clusters are listed. You must select a server where IBM Business Monitor has been installed. If you have more than one server with the same name, be sure to choose the server on the correct node.

   c. To install the application, click **Deploy Monitor Scheduled Services**. The application status box is updated with the location of the installed application, named IBM_WBM_DATA_SERVICES. If this application has been installed to a cluster, the application will appear unavailable until all nodes in the cluster have been synchronized.

   d. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.

   You can view the scheduled services for each installed monitor model by clicking **Applications** > **Monitor services** > **Monitor scheduled services**

7. Optional: If you plan to use the IBM Cognos Business Intelligence service to conduct multidimensional analysis on your dashboards, in the list of optional components, click **Cognos**. The status for the service is displayed. If the service is properly installed, the location of the installed service is listed in the status box. (If you installed IBM Cognos BI with IBM Business Monitor and created a stand-alone profile, the IBM Cognos BI service is already deployed.)

   a. To deploy a new IBM Cognos BI service, select the server or cluster for the IBM Cognos BI service from the list. All available servers and clusters are listed. (The available servers and clusters are shown with asterisks (*)). If you have more than one server with the same name, be sure to choose the server on the correct node.

      Provide a database name to be used for the content store. On DB2 and Microsoft SQL Server, the database name must be different from the MONITOR database name. Provide a database user name and password. If you use the same user name for the content store as for the MONITOR database, you must use the same password. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

      **Note:** The user name and password for the IBM Cognos BI content store database are kept in the Cognos_JDBC_Alias, which allows all database credentials to be maintained in one place. Whenever you start the IBM Business Monitor IBM Cognos BI server, the current values are passed to the IBM Cognos BI configuration to allow IBM Cognos BI access to the content store. Because of this integration, you cannot change the content store user name and password using the IBM Cognos BI Configuration application.
      If administrative security is enabled, you must also provide the IBM Cognos BI administrator user name and password.

Click **Create a New Cognos Service**. The status box is updated with the location of the installed service. If this service has been installed to a cluster, the service will appear unavailable until all nodes in the cluster have been synchronized and restarted. If the deployment takes more time than is provided by the administration console response timeout, you might see a timeout message. Wait a few more minutes before attempting to restart the servers.

b. If you already have an existing version of IBM Cognos BI installed, under Use an existing Cognos service, provide the external dispatcher URI of the IBM Cognos BI server. You can find this URI in the IBM Cognos BI configuration client in **Local Configuration** > **Environment** > **Dispatcher Settings** (for example, `http://my_host:my_port/p2pd/servlet/dispatch/ext`). If administrative security is enabled on the IBM Cognos BI server, you must also provide the IBM Cognos BI administrator user name and password.

   Click **Use an Existing Cognos Service**. The status box is updated with the location of the installed service.

c. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.

8. Optional: If you plan to use the IBM Business Monitor dashboards on mobile devices, you must install the application by completing the following steps. If you do not plan to use the dashboards on mobile devices, you are not required to complete these steps.
   a. In the list of optional components, click **Dashboards for mobile devices**. The status for the application is displayed. If the application is properly installed, the location of the installed application is listed in the status box.
   b. Under **Deploy Dashboards for mobile devices**, select the server or cluster for the dashboards on mobile devices application from the list. All available servers and clusters are listed. You must select a server where IBM Business Monitor has been installed. If you have more than one server with the same name, be sure to choose the server on the correct node.
   c. To install the application, click **Deploy the Dashboards for Mobile Devices**. The application status box is updated with the location of the installed application, named IBM_WBM_MOBILE_DASHBOARD. If this application has been installed to a cluster, the application will appear unavailable until all nodes in the cluster have been synchronized.
   d. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.
9. Optional: If you plan to use the Java Messaging Service (JMS) and Representational State Transfer (REST) event emitter services, you must install the API service applications by completing the following steps. Rather than coding or generating Common Base Events directly, you can then use these event emitter services. You provide the event XML, and the event emitter services receive the event XML and wrap it in a Common Base Event so that IBM Business Monitor can process it.
   a. In the list of optional components, click **Inbound event emitter services (JMS and REST)**. The status for the applications is displayed. If the application are properly installed, the locations of the installed applications are listed in the status box.
   b. Under **Deploy event emitter services**, select the server or cluster for the applications from the list. All available servers and clusters are listed. You must select a server where IBM Business Monitor has been installed. If you have more than one server with the same name, be sure to choose the server on the correct node.
   c. To install the applications, click **Deploy Event Emitter Services**. The application status box is updated with the locations of the installed applications. If the applications have been installed to a cluster, the applications will appear unavailable until all nodes in the cluster have been synchronized.
   d. Return to the configuration page by clicking **IBM Business Monitor configuration** in the breadcrumb listing.
10. Optional: To configure the Representational State Transfer (REST) Services Gateway for widgets for Business Space, complete the following steps.

**Note:** Because the REST Services Gateway is a shared component, you cannot configure it using the configuration wizard. If you create clusters using the deployment environment configuration wizard, or create a stand-alone profile, the REST Services Gateway is configured for you. The REST Services Gateway must be deployed and registered with Business Space before your team can use the widgets in Business Space.

a. In the administrative console, click **Servers** > **Server Types** > **WebSphere application servers** or **Servers** > **Clusters** > **WebSphere application server clusters**.
b. Click the name of your server or cluster.
c. On the Configuration page, under **Business Integration**, click **Rest Services**.

11. Optional: To configure Business Space, complete the following steps.

    **Note:** Because Business Space is a shared component, you cannot configure it using the configuration wizard. If you create clusters using the deployment environment configuration wizard, or create a stand-alone profile, Business Space is configured for you.

    a. In the administrative console, click **Servers** > **Server Types** > **WebSphere application servers** or **Servers** > **Clusters** > **WebSphere application server clusters**.
    b. Click the name of your server or cluster.
    c. On the Configuration page, under **Business Integration**, click **Business Space Configuration**.

12. After you have finished configuring components, synchronize the nodes. In the administrative console, click **System administration > Nodes**, select all of the nodes, and click **Full Resynchronize**. Then stop and restart all of the clusters and servers.

To verify that all applications are correctly installed and configured, log out of the administrative console. Then, log in to the administrative console and navigate to **Servers** > **IBM Business Monitor configuration**. Verify that all items are complete and marked with a green check icon.

If you did not choose to create the messaging engine tables, or did not have permission to create them, the tables must be created manually by a database administrator. See "Creating messaging engine tables manually" in the related links.

If you want to receive events from a CEI event source that is running on a remote server, you must also perform cross-cell configuration. See "Configuring how to receive events" for instructions.

## Configuring the environment using wsadmin commands

Rather than using the configuration wizard, you can configure the IBM Business Monitor environment using the WebSphere command-line administration tool (wsadmin).

The following wsadmin commands are required to configure IBM Business Monitor.

*Table 4. Required wsadmin commands*

| Command | Purpose |
|---|---|
| wbmDeployCEIEventService | Creates and configures the CEI event service that IBM Business Monitor requires to receive and send events. |
| wbmConfigureEventEmitterFactory | Configures the event emitter factory that IBM Business Monitor requires to generate and send events. This command must be run after the wbmDeployCEIEventService command. |
| wbmDeployMessagingEngine | Installs and configures the messaging engine and service integration bus required for IBM Business Monitor. |

*Table 4. Required wsadmin commands (continued)*

| Command | Purpose |
|---|---|
| wbmDeployActionServices | Installs the IBM Business Monitor action services application. This application invokes actions, such as sending dashboard alerts or email notifications, when it receives defined situation events. This command must be run after the wbmConfigureEventEmitterFactory command. |
| wbmDeployScheduledServices | Installs the Monitor scheduled services application that schedules recurring services, such as the data movement service and the key performance indicator (KPI) history for monitor models. |

The following wsadmin commands are optional.

*Table 5. Optional wsadmin commands*

| Command | Purpose |
|---|---|
| wbmDeployCognosService wbmSetCognosDispatcher | Installs a new IBM Cognos Business Intelligence service for multidimensional analysis, or connects to an existing IBM Cognos BI service. |
| wbmSetCognosDatabaseUser wbmSetCognosAdminUser | Changes the passwords for the IBM Cognos BI content store database and the IBM Cognos BI administrator. |
| wbmRemoveCognosService | Removes the IBM Cognos BI service that was installed with IBM Business Monitor. |
| wbmDeployDashboardsForMobileDevices | Installs and configures the application that is required for running the dashboards on mobile devices. |
| wbmDeployEventEmitterServices | Installs and configures the REST event emitter service and the JMS event emitter service applications. The JMS event emitter can asynchronously publish XML events to a Java Messaging Service (JMS) queue without the Common Base Event wrapper, so that XML events can be put on the JMS queue even when IBM Business Monitor services are unavailable. The REST event emitter can synchronously publish events without the Common Base Event wrapper. You define the XSD that describes the structure of the business information, and the REST API generates and sends the event in the correct format for IBM Business Monitor. |
| wbmDeployBPMEmitterService | Installs and configures the IBM Business Process Manager event emitter service application for use by IBM BPM. |
| wbmConfigureQueueBypassDatasource | Creates the data source needed to enable queue bypass communication when IBM Business Monitor is installed in a different cell from the CEI server. |

To run the wsadmin tool, complete the following steps:

1. Open a command prompt, and change directories to the **bin** directory of the deployment manager profile (by default, DMGR01) where WebSphere Application Server is installed, or to the **bin** directory of the stand-alone profile in a single-server environment.
2. Launch **wsadmin** by running one of the following commands:
   - **wsadmin.sh -lang jacl -user <*user_name*> -password <*password*>**
   - **wsadmin.sh -lang jython -user <*user_name*> -password <*password*>**

- **wsadmin.bat -lang jacl -user <*user_name*> -password <*password*>**
- **wsadmin.bat -lang jython -user <*user_name*> -password <*password*>**

3. Run the commands you need. The following example uses Jacl to run the wbmConfigureEventEmitterFactory command and then save the changes:

   ```
   $AdminTask wbmConfigureEventEmitterFactory {-cluster firstCluster}
   $AdminConfig save
   ```

   The following example uses Jython:

   ```
   AdminTask.wbmConfigureEventEmitterFactory('[-cluster firstCluster]')
   AdminConfig.save()
   ```

4. After running the commands, save the changes before exiting wsadmin. To save the changes, use the following syntax:

   ```
   (jacl) $AdminConfig save
   (jython) AdminConfig.save()
   ```

5. In a network deployment environment, synchronize the nodes. In the administrative console, click **System administration > Nodes**, select all of the nodes, and click **Full Resynchronize**. Then stop and restart all of the clusters and servers.

### Interactive mode

When you use an administrative command in interactive mode, you go through a series of steps to collect your input interactively. This process provides a text-based wizard and a similar user experience to the wizard in the administrative console. If you use the **-interactive** parameter, you are prompted to enter each value in turn.

The following examples show how to use this parameter.

```
(jacl) $AdminTask wbmConfigureEventEmitterFactory {-interactive}
(jython) AdminTask.wbmConfigureEventEmitterFactory('-interactive')
```

You can use the **help** command to obtain help for any administrative command.

```
(jacl) $AdminTask help wbmConfigureEventEmitterFactory
(jython) print AdminTask.help ('wbmConfigureEventEmitterFactory')
```

For the details and parameters of the commands, see Configuration commands (wsadmin).

For the Business Space commands, see Commands (wsadmin scripting) for configuring Business Space.

## Configuring the environment manually

You should always use the IBM Business Monitor configuration wizard or deployment environment configuration wizard to configure the IBM Business Monitor environment. This manual information is included to help in advanced or troubleshooting scenarios.

### Configuring the event emitter factory for IBM Business Monitor for z/OS

IBM Business Monitor uses an outbound CEI event service to create and send events. The event service in turn uses an event emitter factory that requires configuration. The preferred way to install the event emitter factory is to use the IBM Business Monitor configuration wizard, the deployment environment configuration wizard, or the wsadmin task. It is also possible to configure the event emitter factory manually.

Complete the following steps from the deployment manager administrative console:

1. In the navigation panel, click **Service integration** > **Common Event Infrastructure** > **Event emitter factories** > **Default Common Event Infrastructure**.
2. Under Additional Properties, click **Event Service Transmission**.
3. Select your event service from the **Event service** list, and click **OK**.

4. Click **Save** to save all changes to the master configuration.
5. In the navigation panel, click **Service integration** > **Common Event Infrastructure** > **Event emitter factories**.
6. Select **cell** for the **Scope**.
7. Click **New**.
8. Type ***factory_name*** for the **Name**. Where *factory_name* can be any name you choose. For example, MonitorEmitterFactory.
9. Type **com/ibm/monitor/MonitorEmitterFactory** for the **JNDI Name**.
10. Under **Event transmission**:
    a. Select the check box **Support event service transmission**.
    b. From the list in the **JNDI name for event service transmission** field, select **Use entry from below**.
    c. In the entry field below the **JNDI name for event service transmission** field, enter one of the following options:
    - Cluster: **cell/clusters/*cluster_name*/com/ibm/events/configuration/bus-transmission/Default**

      Where:

      *cluster_name* represents the cluster where the CEI is deployed.
    - Server: **cell/nodes/*node_name*/servers/*server_name*/com/ibm/events/configuration/bus-transmission/Default**

      Where:

      *node_name* represents the node where the CEI is deployed

      *server_name* represents the server where the CEI is deployed.
11. Clear the **Compatibility mode with previous event service transmission protocol** check box.
12. Click **OK**, and click **Save** to save changes to the master configuration.

## Installing the IBM Business Monitor action services application

The IBM Business Monitor action services application invokes actions, such as sending dashboard alerts or email notifications, when it receives defined situation events emitted by IBM Business Monitor and other applications. Situation events typically indicate business situations that need attention, such as a printer running out of paper or a metric exceeding a certain value.

Before installing monactionmgr.ear, you must enable CEI and the Startup Beans Service on the server where you are installing the action services application.

Complete the following steps to install the action services application using the administrative console:

1. In the navigation panel, click **Applications** > **Application types** > **WebSphere enterprise applications**.
2. Click **Install**.
3. Choose one of the following options for the **Path to the new application**:
   - **Local file system**: Choose this option if the file is on the local system.
   - **Remote file system**: Choose this option if you are accessing the administrative console using a web browser on a different system.
4. Click **Browse**, and browse to select the monactionmgr.ear file, and click **Next**. The EAR files are located in the following directory after installation:

   **monitor_root/installableApps.wbm**

   Where:

   monitor_root represents the directory where IBM Business Monitor is installed
5. On the Select installation options panel, click **Next**.

6. On the Map modules to servers panel, click ***server_name*** or ***cluster_name*** where you want to install the application.
7. Select the check boxes on the rows associated with each module, and click **Apply**.
8. Click **Next**.
9. Review the summary information and click **Finish**.

## Creating the Monitor action services group profile

After you have installed the Monitor action services application, you must create an event group profile to receive events.

Before beginning this task, you must have completed the following tasks:

- Installed the Monitor action services application
- Configured common event infrastructure (CEI) event services for IBM Business Monitor
- Started the deployment manager

Using the administrative console, complete the following steps to create the event group profile:

1. In the navigation panel, click **Service integration** > **Common Event Infrastructure** > **Event service**.
2. Under Additional Properties, click **Event services**.
3. Click **Default Common Event Infrastructure event server**.
4. Under Additional Properties, click **Event groups**.
5. Click **New**.
6. Type **Action Services Group Profile** for the **Event group name**.
7. Type **CommonBaseEvent[extendedDataElements/@name = 'BusinessSituationName']** for the **Event selector string**.
8. Click **Apply**.
9. Under Additional Properties, click **Distribution queues**.
10. Click **New**.
11. Select **jms/ActionManager/queue** from the **Queue JNDI name** drop-down list.
12. Select **jms/ActionManager/QueueConnFactory** from the **Queue connection factory JNDI name**.
13. Click **Apply**.
14. Click **Save** to save changes to master configuration.

## Installing Monitor scheduled services

The Monitor scheduled services application supports multiple services, some of which optimize performance or are used for base processing. You can configure it on the WebSphere Application Server administrative console. You must install this application to schedule recurring services, such as the data movement service and the key performance indicator (KPI) history for monitor models.

Complete the following steps to install the Monitor scheduled services application:

1. In the navigation panel, click **Applications** > **Application types** > **WebSphere enterprise applications**.
2. Click **Install**.
3. Choose one of the following options for the **Path to the new application**:
   - **Local file system**: Choose this option if the file is on the local system.
   - **Remote file system**: Choose this option if you are accessing the administrative console using a web browser on a different system.
4. Click **Browse**, and browse to select the MonitorDataServices.ear file, and click **Next**. The EAR files are located in the following directory after installation:

   **monitor_root/installableApps.wbm**

Where:

monitor_root represents the directory where IBM Business Monitor is installed

5. On the Select installation options panel, click **Next**.
6. On the Map modules to servers panel, click ***server_name*** or ***cluster_name*** where you want to install the application.
7. Select the check boxes on the rows associated with each module, and click **Apply**.
8. Click **Next**.
9. Review the summary information and click **Finish**.

In a network deployment environment, after installing the Monitor scheduled services application, you must create a scheduler resource on the same cluster. Follow the instructions in "Creating and configuring a scheduler resource."

**Creating and configuring a scheduler resource:**

A scheduler resource is a component that drives the scheduler processing by delegating work to the local work manager, which is created at the cell scope during the installation. In a stand-alone server environment, a scheduler resource is created for you during the IBM Business Monitor installation. In a network deployment environment, you must create a scheduler resource on the same server or cluster as the MonitorDataServices.ear file. This topic provides the steps for creating a scheduler resource using the administrative console.

You must first have installed the Monitor scheduled services, following the instructions in the link below.

After installing the scheduled services, use the steps below to create a scheduler resource for a server or cluster.

1. On the administrative console navigation panel, click **Resources** > **Schedulers**.
2. In the **Scope** field, select a server or cluster scope. It must be the same server or cluster as the MonitorDataServices.ear file.
3. Click **New**.
4. In the **Name** field, enter the name to be displayed for the resource, such as DataServicesScheduler.
5. In the **JNDI Name** field, enter `sched/wbm/DataServicesScheduler`.
6. Enter a brief description of this scheduler resource.
7. Optional: Optional. Enter a category to use to classify or group the resource.
8. In the **Data source JNDI name** field, select `jdbc/wbm/MonitorDatabase`.
9. Optional: For the data source alias, choose **Monitor_JDBC_Alias**.
10. In the **Table prefix** field, enter the string prefix to assign to the scheduler tables, including the database schema. This prefix differentiates one scheduler from another which enables them to share the same database. In a typical Monitor environment, the prefix should match the prefix that was used in the Monitor installation DDL, **<*MONITOR_SCHEMA_NAME*>.MONSCHED_**, for example **MONITOR.MONSCHED_<*/MONITOR_SCHEMA_NAME*>**.
11. In the **Poll interval** field, indicate the number of seconds that you want the scheduler to poll the database to look for new work. For IBM Business Monitor, a value of 30 to 60 seconds is recommended.
12. In the **Work manager JNDI name** field, select the work manager, **wm/wbm/ DataServicesWorkManager**.
13. To enable administrative security allowing access only to administrators, click **Use administration roles**.
14. Click **OK** to save this scheduler resource.

## Installing dashboards for mobile devices

You can use IBM Business Monitor dashboards on mobile devices. You must install the application using the WebSphere Application Server administrative console.

Complete the following steps to install the dashboards on mobile devices application:

1. In the navigation panel, click **Applications** > **Application types** > **WebSphere enterprise applications**.
2. Click **Install**.
3. Choose one of the following options for the **Path to the new application**:
   - **Local file system**: Choose this option if the file is on the local system.
   - **Remote file system**: Choose this option if you are accessing the administrative console using a web browser on a different system.
4. Click **Browse**, and browse to select the MobileDashboard.ear file, and click **Next**. The EAR files are located in the following directory after installation:

   **monitor_root/installableApps.wbm**

   Where:

   monitor_root represents the directory where IBM Business Monitor is installed
5. On the Select installation options panel, click **Next**.
6. On the Map modules to servers panel, click ***server_name*** or ***cluster_name*** where you want to install the application.
7. Select the check boxes on the rows associated with each module, and click **Apply**.
8. Click **Next**.
9. Review the summary information and click **Finish**.

After you have installed the application and installed some monitor models, you can access the dashboard for mobile devices using the following web address:

**http://*host_name*:*port_number*/mobile**

Where:

*host_name* represents the fully qualified host name or IP address of the server where the application is installed

*port_number* represents the default port for IBM Business Monitor applications

For the dashboards to work properly on mobile devices, you must configure Business Space. To configure Business Space, you must complete tasks such as enabling the widgets and configuring REST services.

## Installing event emitter services

You can manually install the event emitter services that you use with IBM Business Monitor. Before manually installing event emitter services, you must first create resources for the event emitter services.

**Creating resources for manually installed event emitter services:**

When you manually install event emitter services, you must first create resources. If you do not use the configuration wizard to install the emitter services, or if you deploy more than one instance of the emitter services for performance reasons, you must manually create all required resources for the event emitter services. See the related links. You use the administrative console to create the required resources.

Before you begin this task, you must create the IBM Business Monitor service integration bus (SIB). For instructions, see the related reference.

This topic provides instructions for creating the following required resources:

- JMS destination queue
- JMS error destination queue
- Error queue connection factory
- Queue connection factory
- JMS queue
- JMS error queue
- Activation specification
- Event emitter factory for the REST event emitter service
- Event emitter factory for the JMS event emitter service

**Note:** If you are creating these resources for a JMS emitter for the first time on a server (if the event services were not previously deployed manually on the server or by the configuration wizard), you can choose to use all the default names to simplify installation of the emitter services. In the following steps, the default names are indicated. You can reuse already-defined event emitter factories or create new event emitter factories. Create separate event emitter factories for REST and for JMS.

Use the administrative console to create the resources, and create the resources in the order given.

1. To create the JMS destination queue, complete the following steps:
   a. Select **Service integration** > **Buses**, and click **MONITOR.*cell_name*.Bus**.
   b. Select **Destination resources** > **Destinations**, and then click **New**.
   c. When the **create new destination queue creation** wizard launches, ensure that **Queue** is selected, and click **Next**.
   d. Name the resource `MonitorEventEmitterQueue2`. The default is **MonitorEventEmitterQueue**.
   e. For the description, provide a general description of the queue. For example: `Queue for the Business Monitor server JMS event emitter queue`. Click **Next**.
   f. Select the **Node** where the Bus member resides, click **Next**, and then click **Finish**.
2. To create the JMS error destination queue, repeat Step 1. Name the resource `MonitorEventEmitterErrorQueue2`. The default is **MonitorEventEmitterErrorQueue**. For the description, type `Bus for the Business Monitor server JMS event emitter error queue`.
3. Specify the error queue as the exception destination queue.
   a. Select **Service integration** > **Buses**, and click **MONITOR.*cell_name*.Bus**.
   b. Select **Destination resources** > **Destinations**, and select the destination queue that you created in Step 1.
   c. In the **Exception destination** section, select the **Specify** button, and specify the name of the error queue that you created in Step 2
   d. Click **OK**, and then click **Save**.
4. To create the error queue connection factory, complete the following steps:
   a. Select **Resources** > **JMS** > **Queue connection factories**.
   b. Select the appropriate scope for the new error queue connection factory, and click **New**.
   c. Click **OK** to accept the default messaging provider.
   d. On the **Configuration** tab, type the **Name**, **Description**, and **JNDI name** for the new error queue connection factory, and select the **Bus name**. Click **OK**, and then click **Save**. See the following list items:
      - **Name**: `MonitorEmitterErrorQConnFactory2`
        The default name is **MonitorEmitterErrorQConnFactory**.
      - **Description**: `ErrorQConnFactory for the Business Monitor server JMS event emitter queue`
      - **JNDI name**: `jms/MonitorEventEmitter/ErrorQConnFactory2`
        The default JNDI name is **jms/MonitorEventEmitter/ErrorQConnFactory**.

- **Bus name**: MONITOR.*cell_name*.Bus

e. Specify the Security Settings for a secure environment, and then click **Apply**. The authentication alias for XA recovery is **MonitorBusAuth**. The Container-managed authentication alias is **MonitorBusAuth**.

5. To create the queue connection factory, repeat Step 4 on page 122. Use the following information:
   - **Name**: MonitorEmitterQConnFactory2

     The default name is **MonitorEmitterQueueConnFactory**.
   - **Description**: QConnFactory for the Business Monitor server JMS event emitter queue
   - **JNDI name**: jms/MonitorEventEmitter/QueueConnFactory2

     The default JNDI name is **jms/MonitorEventEmitter/QueueConnFactory**
   - **Bus name**: MONITOR.*cell_name*.Bus

   .
6. To create the JMS queue, complete the following steps:
   a. Select **Resources** > **JMS** > **Queues**.
   b. Select the appropriate scope for the new queue, and click **New**.
   c. Click **OK** to accept the default messaging provider.
   d. On the **Configuration** tab, type the **Name** and **JNDI name** for the new queue, and select the **Bus name** and the **Queue name**. Click **Apply**. See the following list items:
      - **Name**: MonitorEventEmitterQueue2

        The default name is **MonitorEventEmitterQueue**
      - **JNDI name**: jms/MonitorEventEmitter/Queue2

        The default JNDI name is **jms/MonitorEventEmitter/Queue**.
      - **Bus name**: MONITOR.*cell_name*.Bus
      - **Queue name**: Select the JMS destination queue that you created in Step 1 on page 122
7. To create the JMS error queue, repeat Step 6. Use the following information:
   - **Name**: MonitorEventEmitterErrorQueue2

     The default name is **MonitorEventEmitterErrorQueue**
   - **JNDI name**: jms/MonitorEventEmitter/ErrorQueue2

     The default JNDI name is **jms/MonitorEventEmitter/ErrorQueue**
   - **Bus name**: MONITOR.*cell_name*.Bus
   - **Queue name**: Select the JMS error destination queue that you created in Step 2 on page 122
8. To create the activation specification, complete the following steps:
   a. Select **Resources** > **JMS** > **Activation specifications**.
   b. Select the appropriate scope for the new activation specification, and click **New**.
   c. Click **OK** to accept the default messaging provider.
   d. On the **Configuration** tab, type the **Name**, **JNDI name**, and select the **Bus name**, **Destination type**, and **Destination JNDI** for the new activation specification. See the following list items:
      - **Name**: MonitorEventEmitterActivationSpec2

        The default name is **MonitorEventEmitterActivationSpec**
      - **JNDI name**: jms/MonitorEventEmitter/ActivationSpec2

        The default JNDI name is **jms/MonitorEventEmitter/ActivationSpec**.
      - **Bus name**: MONITOR.*cell_name*.Bus
      - **Destination type**: Queue
      - **Destination JNDI**: Select the JMS destination that you created in Step 1 on page 122
   e. Set the **Authentication Alias** to MonitorBusAuth.Click **OK**, and then click **Save**.

9. To create the event emitter factory for the REST event emitter service, follow these steps:
   a. Select **Service integration** > **Common Event Infrastructure** > **Event emitter factories**
   b. Select the appropriate scope for the new event emitter factory, and click **New**.
   c. On the **Configuration** tab, type the **Name** and **JNDI name** for the new event emitter factory. Click **Apply**. See the following list items:
      - **Name**: `EmitterFactoryForREST2`

        The default name is **EmitterFactoryForREST**.
      - **JNDI name**: `com/ibm/monitor/EmitterFactoryForREST2`

        The default JNDI name is **com/ibm/monitor/EmitterFactoryForREST**.
   d. Under Event transmission, select **Support event service transmission**, select **Use entry from below**, and then type `com/ibm/events/configuration/bus-transmission/Default`.
10. To create the event emitter factory for the JMS event emitter service, repeat Step 9. Click **OK**, and then click **Save**. See the following list items:
    - **Name**: `EmitterFactory2`

      The default name is **EmitterFactory**.
    - **JNDI name**: `com/ibm/monitor/EmitterFactory2`

      The default JNDI name is **com/ibm/monitor/EmitterFactory**.
11. Restart your server so that the changes take effect. If you are creating resources in an network deployment (ND) environment, restart the cluster where the resources were created.

**Manually installing event emitter services:**

You can manually install the event emitter services that you use with IBM Business Monitor. When you manually install event emitter services, you can use existing resources or you can create resources for the event emitter services.

If you choose to create resources for the event emitter services, you must create the resources before you manually install event emitter services. See the related link for instructions about creating resources.

**Note:** For increased performance in a network deployment (ND) environment, deploy the IBM_WBM_EMITTER_SERVICES application on the server where the common event infrastructure (CEI) event service is installed. If you have set up clusters, deploy the emitter services in the support cluster along with the CEI event service.

Complete the following steps to manually install event emitter services:

1. In the IBM Business Monitor administrative console, select **Applications** > **Application Types** > **WebSphere enterprise applications**.

   **Note:** If you created resources as described in Creating resources for manually installed emitter services, remember to restart your server before you deploy the application. If you created resources in an ND environment, restart the cluster where the resources were created.
2. Click **Install**.
3. Choose one of the following options for the **Path to the new application**:
   - **Local file system**: Choose this option if the file is on the local system.
   - **Remote file system**: Choose this option if you are accessing the administrative console using a web browser on a different system.
4. Click **Browse**, browse to select the EmitterServices.ear file, and click **Next**. The EAR files are located in the following directory after installation:

   **monitor_root/installableApps.wbm**

   Where:

monitor_root represents the directory where IBM Business Monitor is installed

5. On the Select installation options panel, select **Detailed**, and then click **Next**. On the next panel, click **Continue**.
6. If the emitter services application was already deployed by an administrator or the configuration wizard, create a unique name for your application. For example: *IBM_WBM_EMITTER_SERVICES2*.
   a. On the Map modules to servers panel, click the *server_name* or *cluster_name* where you want to install the application.
7. Select the check boxes on the rows associated with each module, and click **Apply**.
8. Click **Next**.
9. Optional: If you want to use resources that you created and do not want to accept the defaults, you must make changes on the Bind listeners for message-driven beans panel.
   a. For the **Activation Specification Target Resource JNDI name**, specify the JNDI name that you created in Step 8 of Creating resources for manually installed emitter services. The default is *jms/MonitorEventEmitter/ActivationSpec*.
   b. For the **Destination JNDI name**, specify the JNDI name of the JMS Queue (not the Destination queue) that you created in Step 6 of Creating resources for manually installed emitter services. The default is *jms/MonitorEventEmitter/Queue*.
   c. Set the **ActivationSpec authentication alias** to **MonitorBusAuth**.
10. Optional: On the Map resource references to resources panel, you can specify resources that you created, or you can accept the defaults. Then click **Next**.
    a. For the **Target Resource JNDI name for the EventEmitterMDB**, specify the JNDI name that you created in step 9 of Creating resources for manually installed emitter services, or you can use the default. The default is *com/ibm/monitor/EmitterFactory*.
    b. For the **Target Resource JNDI name for the EventEmitterREST**, specify the JNDI name that you created in step 9 of Creating resources for manually installed emitter services, or you can use the default. The default is *com/ibm/monitor/EmitterFactoryForREST*.

       **Note:** After you click **Next**, you might see the following information:

       ```
       ADMA8019E: The resources that are assigned to the application are beyond the deployment target
       scope. Resources are within the deployment target scope if they are defined at the cell, node,
       server, or application level when the deployment target is a server, or at the cell, cluster,
       or application level when the deployment target is a cluster. Assign resources that are within
       the deployment target scope of the application or confirm that these resources assignments are
       correct as specified.
       ```

       This information is not an error. Click **Continue**.
11. Optional: If the emitter services application was already deployed during product installation or deployed manually by an administrator, give the associated context root of this application a unique name.
    a. On the Map context roots for web modules panel, name the associated context root */rest/bpm/events2*. The default is */rest/bpm/events*.
12. Use this step to map users or groups to the eventemitters role. Or you can map all authenticated users by selecting the eventEmitters role and clicking **Map special subjects** and then **All Authenticated in Application's realm**.
    a. On the Map security roles to users or groups panel, select **eventEmitters role**, click **Map special subjects**, and then click **All Authenticated in Application's realm for a secure environment**. If security is not enabled, select **Everyone**.
13. Review the summary information and click **Finish**.
14. Select **Applications** > **Enterprise Applications** > **IBM_WBM_EMITTER_REST_SERVICES**, and click **Start**.

**Using the configuration wizard to install event emitter services:**

You can use the configuration wizard to install the event emitter services for IBM Business Monitor. See the related link.

# Chapter 10. Configuring IBM Business Monitor components

After you have installed IBM Business Monitor, you can configure additional components.

## Configuring IBM Cognos BI

To set up the IBM Cognos Business Intelligence service to conduct multidimensional analysis on your dashboards, you can configure a new IBM Cognos BI service after you install IBM Business Monitor, or you can configure an existing IBM Cognos BI service to use with IBM Business Monitor.

## Configuring a new IBM Cognos BI service

When you install IBM Business Monitor, you can optionally install a new IBM Cognos Business Intelligence service. You can configure the new IBM Cognos BI service in the following ways: create a deployment environment, run the configuration wizard from the administrative console, use the **wbmDeployCognosService** command, or create an IBM Business Monitor stand-alone profile in the Profile Management Tool. You must also create an IBM Cognos BI database and user name for the content store.

IBM Business Monitor copies database drivers and application files to the IBM Cognos BI installation directories during the creation or augmentation of a IBM Business Monitor deployment manager or stand-alone profile. IBM Business Monitor also creates the IBM Cognos BI enterprise application (EAR file) to have it available for deployment of the IBM Cognos BI service.

### Cluster requirements

For cluster members, at least 1 GB of extra disk space is required for IBM Cognos BI because a runtime instance must be created on each cluster member.

It is important to start only one of the cluster members at a time and wait for IBM Cognos BI to initialize fully before starting the next cluster member. IBM Cognos BI requires extra time when it is started for the first time, because the runtime instance must be created and the content store database must be initialized.

Starting another cluster member before the content store is fully initialized can cause corruption to the database. If this corruption occurs, it will be noted in the `cogserver.log` file for the IBM Cognos BI runtime instance. To recover, drop the content store database, re-create the database, and then restart a single cluster member. The DDL script to create the database is located in the `/dbscripts/Cognos` directory on the deployment manager.

### Database requirements

The IBM Cognos BI service requires a separate database for its content store repository (called, by default, the COGNOSCS database). You can create this database while configuring a stand-alone or deployment manager profile, use the database design tool (dbDesignGenerator), or manually create the database using the scripts provided by IBM Business Monitor.

The IBM Cognos BI service creates tables in the IBM Cognos BI content store database the first time it is started. Because the database user provided for accessing the content store database must have privilege to create tables in the database, it is recommended that you create a new database user for the content store database only.

Systems where the IBM Cognos BI server is running must have the database client installed. The WebSphere environment must have access to the client and the client must be configured to connect to

© Copyright IBM Corp. 2005, 2012

the MONITOR database. See the "Database considerations" page and the information for your specific database.

## Security requirements

When IBM Cognos BI is first deployed, the preconfigured group named Everyone belongs to several built-in groups and roles in the IBM Cognos BI namespace, including the **System Administrators** role. You must remove the Everyone group from all built-in groups and roles, and replace it with groups, roles, or users authorized to restrict access to IBM Cognos BI software and administration.

See "Configuring IBM Cognos BI security" for more configuration settings.

When IBM Cognos BI and Business Space are not running on the same cluster member, you must add the IBM Cognos BI host name and port number to the list of trusted servers in IBM Cognos BI. Otherwise, you will not be able to view the pages in Business Space. See step 3 on page 131 in "Configuring IBM Business Monitor and Business Space to use an existing IBM Cognos BI service."

## IBM Cognos BI system compatibility

When you create or augment an IBM Business Monitor deployment manager profile, the configuration files are copied and an enterprise archive (EAR) file is generated for IBM Cognos BI. The IBM Cognos BI EAR file is specific for the platform architecture (operating system and bit mode). When IBM Business Monitor deploys the IBM Cognos BI service, it uses the EAR file that was generated on the deployment manager for all nodes in the cell that are running IBM Cognos BI. To successfully run the EAR file, all nodes must be of the same type. If you have nodes that are of a different type from the deployment manager, you must generate an EAR file on one of the nodes. See "Generating an EAR file for IBM Cognos BI on a custom IBM Business Monitor node."

## Bit modes

All IBM Cognos BI servers are configured to run in the same bit mode as the deployment manager. For example, if the deployment manager is running on a 32-bit platform, all IBM Cognos BI servers are configured in 32-bit mode.

If you want to change the bit mode, complete the following steps for each IBM Cognos BI server:

1. In the administrative console, click **Servers** > **Server types** > **WebSphere application servers** > *server name*. The Configuration panel is displayed.
2. Under Server Infrastructure, expand **Java and Process Management** and click **Process Definition**.
3. Under Additional Properties, click **Environment Entries**. Click **PATH** for each server and update the path settings for the environment variables to point to the correct directory. For 32-bit systems, point to the `bin` directory. For 64-bit systems, point to the `bin64` directory.
4. Synchronize the node and restart the server.

## Locating your runtime IBM Cognos BI root directory

Because IBM Cognos BI configuration settings and binaries are for a single runtime instance, IBM Business Monitor might have to create a new copy for each runtime instance during deployment of the service. IBM Business Monitor checks on startup for updates to the base installation of IBM Cognos BI and applies those to the copy made for each runtime instance. Therefore, if service is required for IBM Cognos BI, only the base installation must be updated.

The copy for each runtime instance is placed under the profile running the IBM Cognos BI service. All configuration, runtime binaries, and log files are kept in unique directories for each runtime instance. The following table shows the location of the IBM Cognos BI root directory for the IBM Cognos BI runtime instance:

*Table 6. Location of the IBM Cognos BI root directory*

| Server type | Directory |
|---|---|
| First stand-alone server | **app_server_root/cognos** |
| Second stand-alone server | **profile_root/***profile_name***/cognos/***server_name* |
| Cluster member server | **profile_root/***profile_name***/cognos/***server_name* |

## Updating the IBM Cognos BI configuration

IBM Business Monitor saves updates to the IBM Cognos BI configuration each time the AdminTask **wbmDeployCognosService** command is run. For example, if the security setting changes from Federated to Stand-alone LDAP, or the Content Manager database settings change, run the **wbmDeployCognosService** command to reconfigure IBM Cognos BI, based on the parameters you pass to the command as well as the current WebSphere settings for the database and user registry.

The changes to the runtime instance of the IBM Cognos BI configuration are made during the server startup based on the changes from **wbmDeployCognosService**. IBM Business Monitor checks for changes to the IBM Cognos BI configuration each time the server is started.

Run the **wbmDeployCognosService** command for the following types of changes to WebSphere:

- User registry changes
- Database changes to either IBM Business Monitor or IBM Cognos BI
- Hostname, IP address, and HTTP port address changes

**Important:** Updates made to the IBM Cognos BI configuration using **wbmDeployCognosService** will be ignored if the IBM Cognos BI Configuration application program has been used to make manual changes to the configuration. Once you have used the IBM Cognos BI Configuration application program, you must continue to use it to make changes.

Run the **wbmSetCognosDatabaseUser** command for the following types of changes (or edit the Cognos_JDBC_Alias WebSphere authorization alias directly):

- IBM Cognos BI Content Store database user name or password

Run the **wbmSetCognosAdminUser** command for the following types of changes (or edit the Cognos_Admin_Alias WebSphere authorization alias directly)

- IBM Cognos BI administrative user name or password

## Manually updating the IBM Cognos BI configuration

When the IBM Business Monitor preconfigured configuration settings for IBM Cognos BI are not sufficient for complex configurations, you must manually configure IBM Cognos BI using the IBM Cognos BI Configuration application. Use the IBM Cognos BI Configuration application to set the host and port addresses of systems running Business Space to the valid domains or host settings of the IBM Cognos BI firewall settings.

For each unique configuration, there is a unique start script

- Windows `cogconfig.bat`
- Linux UNIX `cogconfig.sh`

The script is located in one of the following directories:

- *cognos_installation_root*`/bin` for 32-bit servers
- *cognos_installation_root*`/bin64` for 64-bit servers

Use the table above to find the *cognos_installation_root* directory.

For each unique configuration, there is a unique start script `cogconfig.bat` or `cogconfig.sh` located in the *cognos_installation_root*`/bin` for 32-bit servers or the *cognos_installation_root*`/bin64` for 64-bit servers. Use the table above to find the *cognos_installation_root* directory.

If there is a problem starting the script because Java is not found, run a command similar to the following to set the environment to locate the version of Java used with your WebSphere server:

- Windows SET JAVA_HOME=C:\WAS70\java
- Linux UNIX export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java

**Important:** Do not run the IBM Cognos BI Configuration application until after the IBM Cognos BI server has been started at least once. The first startup copies the configuration (and the binaries unless the first stand-alone server is starting), and also creates the encryption keys and encrypts the passwords within the configuration.

**Tip:** After the IBM Cognos BI configuration has been saved using the IBM Cognos BI Configuration application, IBM Business Monitor no longer checks for changes to the IBM Cognos BI configuration. However, IBM Business Monitor continues to update the user names and passwords such that you only need to make changes to these in one place (for example, using the WebSphere administrative console to change the authorization alias). IBM Business Monitor updates the IBM Cognos BI configuration during server startup with the name and password from the **Cognos_JDBC_Alias** WebSphere security alias. If you are using the WebSphere stand-alone LDAP repository, changes to the LDAP access are updated in the IBM Cognos BI configuration.

If you need to use the IBM Cognos Administration client, it is located at `http://`*host_name*`:`*port_number*`/p2pd/servlet/dispatch/ext`.

## Manually setting the IBM Cognos BI address that IBM Business Monitor uses

Use the **`wbmSetCognosDispatcher`** command to set the address of a remote or an existing IBM Cognos BI service, or to modify the address of a locally installed IBM Cognos BI service. To allow single sign-on for interactions between IBM Cognos BI and IBM Business Monitor, the IBM Cognos BI address should end with `/ext` (the full IBM Cognos BI external dispatcher address).

After changing the address, restart all IBM Business Monitor servers.

## Generating an EAR file for IBM Cognos BI on a custom IBM Business Monitor node

When you create or augment an IBM Business Monitor deployment manager profile, the enterprise archive (EAR) file that is generated for IBM Cognos Business Intelligence is specific for the operating system and bit mode. To successfully run the EAR file, all nodes must be of the same type. If you have nodes that are of a different type from the deployment manager, you must generate an EAR file on one of the nodes.

To generate an EAR file on a custom IBM Business Monitor node, complete the following steps:

1. Copy the following files from IBM Business Monitor directories to IBM Cognos BI installation directories.

   **Important:** You must rename some of the files (as shown in the table) to replace existing files.

| Copy from (location and file name) | Copy to (location and file name) |
|---|---|
| app_server_root/scripts.wbm/cognos/application.xml | app_server_root/cognos/war/p2pd/application.xml.template |

| Copy from (location and file name) | Copy to (location and file name) |
| --- | --- |
| app_server_root/scripts.wbm/cognos/web.xml | app_server_root/cognos/webapps/p2pd/WEB-INF/web.xml.withCM |
| app_server_root/scripts.wbm/cognos/ibm-web-ext.xmi | app_server_root/cognos/webapps/p2pd/WEB-INF/ibm-web-ext.xmi |
| app_server_root/installableApps.wbm/monAuthProvider.jar | app_server_root/cognos/webapps/p2pd/WEB-INF/lib/monAuthProvider.jar |

2. Open a command prompt in app_server_root/cognos/war/p2pd.
3. Run the following command:

   Windows **build.bat ear**

   Linux UNIX **build.sh ear**

   This command creates a WebSphere EAR file called p2pd.ear in the IBM Cognos BI root directory. Building the EAR file might take several minutes.
4. Copy the new p2pd.ear file to the deployment manager, replacing the existing file in app_server_root/cognos.
5. Deploy the IBM Cognos BI service.

## Configuring IBM Business Monitor and Business Space to use an existing IBM Cognos BI service

If you already have IBM Cognos Business Intelligence installed, you can use your existing IBM Cognos BI service with IBM Business Monitor. You can connect to your existing IBM Cognos BI service in the following ways: run the IBM Business Monitor configuration wizard from the administrative console, use the **wbmSetCognosDispatcher** command, or create a stand-alone profile in the Profile Management Tool. You must then perform some configuration tasks.

After you have connected IBM Business Monitor to your IBM Cognos BI server, you must perform additional steps to set up Business Space and to handle your data services.

**Important:** The remote IBM Cognos BI must be running on a WebSphere Application Server, and when administrative security is enabled, the user repository must be the same on the IBM Business Monitor server and the IBM Cognos BI server.

Make sure that the database client is running and has access to the IBM Business Monitor database on the remote IBM Cognos BI server. Also be sure the IBM Business Monitor database has been cataloged with the remote IBM Cognos BI server with the same name as the catalog entry on the IBM Business Monitor server.

If you created a deployment environment from the administrative console, a new IBM Cognos BI was installed for you. To remove it, use the **wbmRemoveCognosService** command. (If you ran the **wbmSetCognosDispatcher** command before creating a deployment environment, the IBM Cognos BI service was not deployed and therefore does not require removal.)

To set up Business Space to work with your existing IBM Cognos BI, complete the following steps:

1. Configure single sign-on between the WebSphere Application Server running Business Space and the WebSphere Application Server running IBM Cognos BI. See Enabling single sign-on.
2. Configure IBM Cognos BI for single sign-on. See Configuring an existing IBM Cognos BI service for single sign-on.
3. Add the IBM Cognos BI host name and port number to the list of trusted servers in IBM Cognos BI. Otherwise, you will not be able to view the pages in Business Space.

a. Open the IBM Cognos BI Configuration client. To open the client, run the `cogconfig.bat` or `cogconfig.sh` file located in *cognos_installation_root*`/bin` for 32-bit servers or *cognos_installation_root*`/bin64` for 64-bit servers.
b. Select **Local Configuration** > **Security** > **IBM Cognos Application Firewall**.
c. Click the pencil icon next to **Valid domains or hosts** and add the IBM Cognos BI host and port number configured in the endpoint from Business Space. For example, add `lc2d266009.example.com:9080`. If you have multiple hosts, click **Add** to add more entries.
d. Click **OK**. Click **Save**.
e. Restart the server that is running IBM Cognos BI.

4. Because Business Space end points for IBM Cognos BI are configured when the IBM Cognos BI remote URL is configured, verify that the custom properties of the **Mashups Endpoints** resource environment provider are correct:
   a. From the WebSphere administrative console, click **Resources**.
   b. Verify the following custom properties for the **Mashups Endpoints** resource environment provider:

      ```
      {com.ibm.cognos}cognosServiceRootId.url
      {com.ibm.cognos}cognosDispatcherRootId.url
      {com.ibm.cognos}cognosWebContentRootId.url
      ```

5. If the properties you checked in step 4 are not correct, complete the following steps:
   a. Update the following service endpoint file.

      *install_root*`/BusinessSpace/registryData/WBM/endpoints/cognosEndpoints.xml`In each of the three **<tns:url>** sections, add the IBM Cognos BI server host name and port at the beginning of the line.

      For example, if your host name is **lc2d266009.example.com** and your port number is **9080**, the completed file would look like:

      ```
      <tns:Endpoint>
      <tns:id>{com.ibm.cognos}cognosServiceRootId</tns:id>
      <tns:type>{com.ibm.cognos}cognosServiceRootId</tns:type>
      <tns:version>1.0.0.0</tns:version>
      <tns:url>http://lc2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
      <tns:description>Location of backing services for Cognos widgets</tns:description>
      </tns:Endpoint>

      <tns:Endpoint>
      <tns:id>{com.ibm.cognos}cognosDispatcherRootId</tns:id>
      <tns:type>{com.ibm.cognos}cognosDispatcherRootId</tns:type>
      <tns:version>1.0.0.0</tns:version>
      <tns:url>http://lc2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
      <tns:description>Location of Cognos Dispatcher</tns:description>
      </tns:Endpoint>

      <tns:Endpoint>
      <tns:id>{com.ibm.cognos}cognosWebContentRootId</tns:id>
      <tns:type>{com.ibm.cognos}cognosWebContentRootId</tns:type>
      <tns:version>1.0.0.0</tns:version>
      <tns:url>http://lc2d266009.example.com:9080/p2pd/servlet/</tns:url>
      <tns:description>Location of Cognos web content</tns:description>
      </tns:Endpoint>
      </tns:BusinessSpaceRegistry>
      ```

      For more information about modifying the endpoints files, see Enabling Business Space widgets for cross-cell environments.
   b. Run the **updateBusinessSpaceWidgets** command for the `cognosEndpoints.xml` file. Follow the instructions in Enabling Business Space widgets for cross-cell environments.

## Configuring IBM Cognos BI with WebSphere Portal

If you are using IBM Cognos Business Intelligence with WebSphere Portal, you must update the **ProxyServlet_Servlet** section of the `web.xml` file.

For complete information about configuring Business Space to work with WebSphere Portal, see "Configuring widgets to work with WebSphere Portal."

1. Export the WebSphere Portal enterprise archive (EAR) file, `wps.ear`, according to your network configuration. If you have a cluster environment, the WebSphere Portal EAR file must be exported from the WebSphere Application Server Network Deployment machine.
   a. At a command line, change to the *application_server_profile_root*`/bin` directory.
   b. Run the following command to export the `wps.ear` file to a temporary directory (make sure that all commands are entered on one line):
      - Windows **wsadmin.bat -user *admin_user_id* -password *admin_password* -c "$AdminApp export wps *directory*/wps.ear"**
      - Linux UNIX **./wsadmin.sh -user *admin_user_id* -password *admin_password* -c '$AdminApp export wps *directory*/wps.ear'**

      where *admin_user_id* is the administrator's user ID, *admin_password* is the administrator's password, and *directory* is the temporary directory.
2. Create the `/wps_expanded` subdirectory. Use the **EARExpander** scripting tool to expand the contents of the exported EAR file (make sure that all commands are entered on one line).
   - Windows **EARExpander.bat -ear *directory*\wps.ear -operationDir *directory*\wps_expanded -operation expand**
   - Linux UNIX **./EARExpander.sh -ear *directory*/wps.ear -operationDir *directory*/wps_expanded -operation expand**
3. Make a backup copy of *directory*`/wps_expanded/wps.war/WEB-INF/web.xml`.
4. Update *directory*`/wps_expanded/wps.war/WEB-INF/web.xml`.
   a. Open `web.xml`.
   b. Find the following section:

```
<servlet id="ProxyServlet_Servlet">
   <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
</servlet>
```

   c. Replace the section with the following text:

```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
  <init-param>
    <param-name>useCtxPathForCookies</param-name>
    <param-value>true</param-value>
  </init-param>
</servlet>
```

5. Delete the original `wps.ear` file from the directory where you initially exported it.
6. Use the **EARExpander** command to collapse the EAR file directory back into an EAR file.
   - Windows **EARExpander.bat -ear *directory*\wps.ear -operationDir *directory*\wps_expanded -operation collapse**
   - Linux UNIX **./EARExpander.sh -ear *directory*/wps.ear -operationDir *directory*/wps_expanded -operation collapse**
7. Use the wsadmin command to update the WebSphere Portal EAR file.

   **Note:** If you have a managed cell (with or without a cluster), perform this step on the deployment manager machine.

- Windows **wsadmin.bat -user** *admin_user_id* **-password** *admin_password* **-c "$AdminApp install** *directory*/**wps.ear {-update -appname wps -nodeployejb}"**
- Linux UNIX **./wsadmin.sh -user** *admin_user_id* **-password** *admin_password* **-c '$AdminApp install** *directory*/**wps.ear {-update -appname wps -nodeployejb}'**

where *admin_user_id* is the administrator's user ID, *admin_password* is the administrator's password, and *directory* is the temporary directory.

8. Restart WebSphere Portal server. In a cluster configuration, restart the cluster.
9. Add the IBM Cognos BI host name and port number to the list of trusted servers in IBM Cognos BI. Otherwise, you will not be able to view the pages in Business Space.
   a. Open the IBM Cognos BI Configuration client. To open the client, run the `cogconfig.bat` or `cogconfig.sh` file located in *cognos_installation_root*`/bin` for 32-bit servers or *cognos_installation_root*`/bin64` for 64-bit servers.
   b. Select **Local Configuration** > **Security** > **IBM Cognos Application Firewall**.
   c. Click the pencil icon next to **Valid domains or hosts** and add the IBM Cognos BI host and port number configured in the endpoint from Business Space. For example, add `lc2d266009.example.com:9080`. If you have multiple hosts, click **Add** to add more entries.
   d. Click **OK**. Click **Save**.
   e. Restart the server that is running IBM Cognos BI.

## Configuring the reporting data source in IBM Cognos BI

When you publish cube packages for your first monitor model, a reporting data source named WBMONITOR_DB is automatically created in IBM Cognos BI. The WBMONITOR_DB data source is used to connect to the MONITOR database for dimensional reporting.

The WBMONITOR_DB data source is configured based on the values copied from the WebSphere Application Server JDBC data source named Monitor_database.

If you cannot publish cube packages because of database connectivity issues, or if you change the user name or password for the IBM Business Monitor database, you must reconfigure the WBMONITOR_DB data source connection using the IBM Cognos Administration client. Alternatively, you can delete the WBMONITOR_DB data source in the IBM Cognos Administration client and republish a cube package from the IBM Business Monitor administrative console, using the Manage Cognos Cubes page, to automatically regenerate the WBMONITOR_DB data source based on the latest configuration values in the WebSphere Application Server JDBC data source named Monitor_database.

1. Start the IBM Cognos Administration client at `http://`*host_name*`:`*port_number*`/p2pd/servlet/dispatch/ext`.
2. Go to **IBM Cognos Administration** > **Configuration** > **Data Source Connections** > **WBMONITOR_DB**. From there, you can configure and test the connection, and edit the user name and password.

   **Tip:** When you are testing the WBMONITOR_DB connection, you should see two **Succeeded** messages.
   - The first message is of the type "IBM DB2 / Compatible" (or "Oracle / Compatible" or "SQL Server / Compatible"). This message is for the connection that uses the native database client. This connection is required to publish cube packages.
   - The second message is of the type " / Dynamic." This message is for the Type 4 JDBC connection. This connection is required to run IBM Cognos BI reports.

   If either of these connection types show **Failed**, edit the respective configuration or sign-on information and retest. You can safely ignore failures for other connection types.

## Configuring IBM Business Monitor widgets for WebSphere Portal

IBM Business Monitor no longer provides portlet-based dashboards. However, your IBM Business Monitor widgets can still be displayed in WebSphere Portal.

To display widgets in WebSphere Portal, complete the following high-level steps:

1. Configure Business Space.
2. Configure widgets to work with WebSphere Portal.
3. Configure IBM Cognos Business Intelligence to work with WebSphere Portal.

## Configuring how to receive events

You can configure how events flow from applications to the Common Event Infrastructure (CEI) as well as how they flow from CEI to IBM Business Monitor.

## Asynchronous event considerations

The flow from an emitting application to the common event infrastructure (CEI) can be synchronous or asynchronous. With synchronous event transmission, an application waits for successful event delivery before proceeding with the rest of its transaction. With asynchronous event transmission, an application places events on a queue and proceeds with processing.

When you use asynchronous event transmission, you can minimize the impact on the emitting application, which might be important when monitoring mission-critical applications. However, with asynchronous event transmission, events can be received by a monitor model in a different order than they occurred in the emitting application.

For models where event order is important, incorrect event sequence order can result in model processing exceptions and incorrectly calculated data. If you need the order of events to be guaranteed, make sure that the application that is emitting events to IBM Business Monitor uses synchronous event emission, or define an event sequence path in the monitor model to provide information about the event processing order.

One way to tell whether the events are being emitted asynchronously is to check the administrative console under **Service integration** > **Common Event Infrastructure** > **Event emitter factories**. Select the emitter factory, which might be named something like **Default Common Event Infrastructure emitter**. The panel that is displayed has an Event transmission area with settings that control how events are emitted. JMS transmission is asynchronous and event service transmission is synchronous.

If you decide to use asynchronous event emission and it is important that the events be processed in the order in which they were produced, define an event sequence path in the monitor model. For more information about how to define event sequence paths, see the related links.

### Configuring authorization for asynchronous event delivery

If you are planning to receive events that are emitted from an application that uses an event emitter factory with asynchronous delivery, and you did not use the deployment environment configuration wizard or the **wbmDeployCEIEventService** AdminTask to set up your environment, you must configure the IBM Business Monitor server to communicate with the common event infrastructure (CEI) server.

If you used the deployment environment configuration wizard or the **wbmDeployCEIEventService** AdminTask to set up your environment, this configuration is done for you. You must perform this task to configure the authorization information for JMS only if you are configuring your own CEI server or using a non-default event emitter factory rather than the Default Common Event Infrastructure emitter.

Before you begin this task, you must log in to the WebSphere Application Server administrative console. If you are using a remote CEI server and using the queue-based method to receive events, ensure that

you have configured the service integration bus links before beginning this task. See the related task about "Configuring queue-based event management in a multiple-cell environment."

As an alternative to using the administrative console, you can run the wsadmin task **setEventServiceJmsAuthAlias** to perform the steps that are provided in this topic.

Using the WebSphere Application Server administrative console, complete the following steps:

1. Specify the authorization aliases for the queue connection factory.
   a. In the navigation panel, click **Resources** > **JMS** > **Queue connection factories**.
   b. Click **CommonEventInfrastructure_QueueCF** in the list of queue connection factories.
   c. In the Security Settings section, select an alias from the **Authentication alias for XA recovery** list. The alias must have a user that has a bus connector role for the CEI bus. (In **Service Integration** > **Buses**, click the **Security** column for the bus that is described as **CommonEventInfrastructure Bus**.)
   d. Select an alias from the **Container-managed authentication alias** list. Typically you can select the same alias as in the previous substep.
   e. Click **OK** and save your changes to the master configuration.
2. Specify an authorization alias for the activation specification.
   a. In the navigation panel, click **Resources** > **JMS** > **Activation specifications**.
   b. Click **CommonEventInfrastructure_ActivationSpec** in the list of activation specifications.
   c. In the Security Settings section, select an alias from the **Authentication alias** list.
   d. Click **OK** and save your changes to the master configuration.
3. Specify the authorization aliases for the topic connection factories.
   a. In the navigation panel, click **Resources** > **JMS** > **Topic connection factories**.
   b. Click **CommonEventInfrastructure_AllEventsTopicCF** in the list of topic connection factories.
   c. In the Security Settings section, select an alias from the **Authentication alias for XA recovery** list. The alias must have a user that has a bus connector role for the CEI bus. (In **Service Integration** > **Buses**, click the **Security** column for the bus that is described as **CommonEventInfrastructure Bus**.)
   d. Select an alias from the **Container-managed authentication alias** list. Typically you can select the same alias as in the previous substep.
   e. Click **OK** and save your changes to the master configuration.

## Receiving events from CEI

In IBM Business Monitor, you can choose to receive events from the inbound Common Event Infrastructure (CEI) server using two different transport types: JMS (queue-based) and table-based (also known as queue bypass).

Queue-based event delivery uses Java Messaging Service (JMS) to deliver events from CEI to the monitor model. Table-based event delivery (formerly known as queue bypass) uses a database table to deliver events from CEI to the monitor model.

With table-based event delivery, the work can be distributed among multiple cluster members. Additionally, the event flow skips the JMS queue of the monitoring model and directs all events into the event database table of the model. For most environments, this method improves performance by avoiding a persistence step that is required by the JMS queue. Other benefits of the table-based methods are that you no longer have to configure the service integration bus and link when receiving events from a remote cell, and you can rebuild earlier models to use this method.

## Receiving events using table-based event delivery

You can configure your common event infrastructure (CEI) event service to send the events to the event database table for the monitor model. You do not need to configure the service integration bus link and its associated resources. Bypassing the JMS queue improves performance by eliminating an additional persistence step that is required for the queue.

When you use table-based event delivery in IBM Business Monitor 7.5, the work can be distributed among multiple cluster members. For most environments, this method improves performance and simplifies the system configuration.

- **Pre-6.2 models**: Table-based event delivery is not supported. To use this method for monitor models from a version earlier than 6.2, you must first upgrade the monitor model using the Business Monitor development toolkit. Change the version number, generate a new EAR file, and deploy a new version of the monitor model. If you choose not to upgrade the model, you must use queue-based event delivery.
- **Version 6.2 and 7 models**: These models can use the table-based method (formerly known as queue bypass). If you want to exploit the scalability enhancements of version 7.5, you must upgrade the monitor model using a version 7.5 Business Monitor development toolkit.
- **Version 7.5 models**: These models can take advantage of the scalability enhancements if you use table-based event delivery.

**Restriction:** If you are using SQL Server as the database, you cannot use the table-based event delivery method unless the emitting application is running on WebSphere Application Server 7.0 (or Process Server 7.0) or later. You must use the queue-based method.

You can enable the table-based method in a single-cell or multiple-cell environment. Choose the following task depending on your environment to complete the configuration for this method.

**Configuring table-based event delivery in a single-cell environment:**

If you have a single-server (stand-alone) environment or you have IBM Business Monitor version 7.0 or later (or version 7.0.0.3 for z/OS) or later installed on every node in the cell, then there are no further steps required to receive events. If the common event infrastructure (CEI) event service is deployed to a node in the cell without IBM Business Monitor or Process Server, then you must install the IBM Business Monitor JAR files for routing events on that CEI node.

Process Server version 7.0 and later on distributed platforms (and Process Server version 7.0.0.3 and later on z/OS platforms) provides the files needed to support remote event emission. If you are using an earlier version of Process Server, complete the following steps to configure table-based event delivery in a single-cell environment.

1. In the **app_server_root/scripts.wbm/crossCell** directory of the local IBM Business Monitor server installation, locate the appropriate file depending on your operating system and the version of WebSphere Application Server that the CEI event service is running on.
   - `monitorCommunicationWithWAS70BasedCells.tar`, `monitorCommunicationWithWAS61BasedCells.tar`, or `monitorCommunicationWithWAS60BasedCells.tar`.
   - `monitorCommunicationWithWAS70BasedCells.zip`, `monitorCommunicationWithWAS61BasedCells.zip`, or `monitorCommunicationWithWAS60BasedCells.zip`.
2. Copy the appropriate file to the **app_server_root/plugins** directory on every WebSphere Application Server installation in the remote node that hosts a CEI target and does not have IBM Business Monitor or Process Server version 7.0 (or version 7.0.0.3 for z/OS) or later installed, and extract the contents.
3. On each WebSphere Application Server installation where you extracted the contents of the file:
   a. Shut down all Java virtual machines (JVMs) that are using **app_server_root/java/bin/java**, including node agents, servers, deployment managers, and wsadmin prompts.

b. Run **profile_root/bin/osgiCfgInit** for every profile on the WebSphere Application Server installation.
c. Restart all node agents and servers.

**Configuring table-based event delivery in a multiple-cell environment:**

If your IBM Business Monitor is installed in a different cell from the CEI event service, you must complete additional configuration steps to enable the communication between the cells.

For secure environments, before performing this task, ensure that the following tasks have been completed:

- If security is enabled in either the remote or local cell, it must be enabled in both.
- If security is enabled, you must enable server-to-server trust (SSL) between the remote CEI server and the local IBM Business Monitor server (see Configuring server-to-server SSL in multiple-cell environments).
- LTPA keys must be shared across cells and the cells must have the same ID (see Sharing LTPA keys).
- The **Use identity assertion** setting must be enabled in the local cell and the remote cell (see Enabling identity assertion).

In a multiple-cell environment, if IBM Business Monitor is not installed on the remote cell that is emitting events, you must configure the deployment manager and CEI servers in the remote cell so that they can emit events to the tables. Process Server version 7.0 and later on distributed platforms (and Process Server version 7.0.0.3 and later on z/OS platforms) provides the files needed to support remote event emission. Previous versions of Process Server do not provide these files automatically. Consequently, the instructions are slightly different depending on whether the remote cell that is emitting events is a distributed cell that has Process Server version 7.0 (version 7.0.0.3 for z/OS) or later installed.

To configure table-based event delivery across multiple cells, complete the following steps:

- If Process Server version 7.0 (version 7.0.0.3 for z/OS) or later is **not** installed in the remote cell (the cell without IBM Business Monitor):
  1. In the **app_server_root/scripts.wbm/crossCell** directory of the local IBM Business Monitor server installation, locate the appropriate file depending on your operating system and the version of WebSphere Application Server that the CEI event service is running on.
     - `monitorCommunicationWithWAS70BasedCells.tar` or `monitorCommunicationWithWAS61BasedCells.tar`.
     - `monitorCommunicationWithWAS70BasedCells.zip` or `monitorCommunicationWithWAS61BasedCells.zip`.
  2. Copy the appropriate file to the **app_server_root/plugins** directory of the remote deployment manager and extract the contents.
  3. Copy the same file to the **app_server_root/plugins** directory on every WebSphere Application Server installation in the remote cell that hosts a CEI target and does not have IBM Business Monitor or Process Server version 7.0 (or version 7.0.0.3 for z/OS) or later, and extract the contents.
  4. On each WebSphere Application Server installation where you extracted the contents of the file:
     a. Shut down all Java virtual machines (JVMs) that are using **app_server_root/java/bin/java**, including node agents, servers, deployment managers, and wsadmin prompts.
     b. Run **profile_root/bin/osgiCfgInit** for every profile on the WebSphere Application Server installation.
     c. Restart all node agents and servers.
  5. On the remote deployment manager or stand-alone server, run the **wbmConfigureQueueBypassDatasource** wsadmin command. See Table-based CEI across multiple cells for an example and list of parameters for this command. After you run the command and save the configuration changes, restart the remote deployment manager or stand-alone server.

- If Process Server version 7.0 (or version 7.0.0.3 for z/OS) or later **is** installed in the remote cell:
  1. On the remote deployment manager or stand-alone server, run the **wbmConfigureQueueBypassDatasource** wsadmin command. See Table-based CEI across multiple cells for an example and list of parameters for this command.
  2. After you run the command and save the configuration changes, restart the remote deployment manager or stand-alone server.

When you deploy a monitor model with a remote CEI, you need to select the **Remote** CEI location option, as described in the step entitled "Select Monitor model CEI options" in the topic Deploying monitor models.

**If you are running a CEI server on z/OS**: After you complete the table-based CEI configuration, when you deploy a monitor model, the following error is recorded in the CEI logs on z/OS:

```
CEI61Configur E
com.ibm.wbimonitor.observationmgr.spi.impl.CEI61RemoteConfigurationSessionImpl reloadCEIConfig(String[]
eventServerAppNames) CWMRT7314E: Error while trying to reload the CEI configuration.
```

To complete the CEI configuration, complete the following steps:

1. Restart the CEI server or cluster (for the emitting CEI on z/OS).
2. On the IBM Business Monitor deployment manager, run the **confirmCEIServerReboot(String modelID)** method of the Lifecycle Services MBean to indicate that CEI has been restarted. To run the command from a wsadmin prompt, complete the following steps:
   a. Establish a connection to the Lifecycle Services MBean:
      ```
      wsadmin> set ls [$AdminControl completeObjectName type=LifecycleServices,*]
      ```
   b. Confirm that CEI has been restarted:
      ```
      wsadmin> $AdminControl invoke $ls confirmCEIServerReboot { "<model ID>"}
      ```

## Receiving events using queue-based event delivery

To receive events using the Java Messaging Service (JMS) queues, you do not need to perform any additional steps unless you want to enable communication between the IBM Business Monitor server and a remote CEI server. You must use the queue-based method for event management if you are using a monitor model that was created using IBM Business Monitor 6.1 in an IBM Business Monitor 8.0 environment without upgrading your monitor model.

You can use queue-based event management in a single-cell or multiple-cell environment. If your CEI server is in a remote cell to the cell where IBM Business Monitor is installed, then you must complete additional configuration steps to enable the communication across the two cells.

**Configuring queue-based event delivery in a single-cell environment:**

If your IBM Business Monitor is installed in the same cell as the CEI event service, and you are using the queue-based method to receive events, there are no further steps to take. The required JAR files were copied to the correct folders and the service integration bus was created when IBM Business Monitor was installed.

**Configuring queue-based event delivery in a multiple-cell environment:**

If your IBM Business Monitor is installed in a different cell from the CEI server, you must complete additional configuration steps to enable the communication between the cells. To receive events from the JMS queue in this cross-cell environment, you must configure IBM Business Monitor server to receive common event infrastructure (CEI) events from a remote CEI server.

Before performing this task, verify that the following items have been completed:

- The remote CEI service has been deployed and configured.

- The service integration bus for the local IBM Business Monitor server has been created.

For secure environments, you must also ensure that the following tasks have been completed:
- If security is enabled in either the remote or local cell, it must be enabled in both.
- If security is enabled, you must enable server-to-server trust (SSL) between the remote CEI server and the local IBM Business Monitor server (see Configuring server-to-server SSL in multiple-cell environments).
- LTPA keys must be shared across cells and the cells must have the same ID (see Sharing LTPA keys).
- The **Use identity assertion** setting must be enabled in the local cell and the remote cell (see Enabling identity assertion).

To configure the queue-based method of event management, you must install the cross-cell files, create the remote service integration bus, and create the link between the local and remote buses. Process Server version 7.0 and later on distributed platforms (and Process Server version 7.0.0.3 and later on z/OS platforms) provides the files needed to support remote event emission.

To configure queue-based event management across multiple cells, complete the following steps:

**Important:** If Process Server version 7.0 (or version 7.0.0.3 for z/OS) or later is installed in the remote cell, you can skip steps 1-3 and go directly to step 4.

1. In the **app_server_root/scripts.wbm/crossCell** directory of the local IBM Business Monitor server installation, locate the appropriate file depending on your operating system and the version of WebSphere Application Server that the CEI server is running on.

   `monitorCommunicationWithWAS70BasedCells.tar`, `monitorCommunicationWithWAS61BasedCells.tar`, or `monitorCommunicationWithWAS60BasedCells.tar`.

   `monitorCommunicationWithWAS70BasedCells.zip`, `monitorCommunicationWithWAS61BasedCells.zip`, or `monitorCommunicationWithWAS60BasedCells.zip`.
2. Copy the appropriate file to the **app_server_root/plugins** directory of the remote CEI server (either the stand-alone server or the remote deployment manager) and extract the contents.
3. From the **app_server_root/bin** directory on the remote CEI server, run the appropriate command to configure the application server or process server to recognize the .jar file: **osgiCfgInit.bat** or **osgiCfgInit.sh.**
4. From the **app_server_root/scripts.wbm/crossCell** directory of the local IBM Business Monitor server installation, choose one of the methods below to run the service integration bus cross-cell configuration utility. For more information about this utility, see the related links.
   - To run the command interactively, enter:

     **configRemoteMonitorBus.sh**

     **configRemoteMonitorBus.bat**
   - To run the command using a properties file, review the **configRemoteMonitorBus.props** file and change any necessary properties. The **configRemoteMonitorBus.props** file is an example properties file that is located in the **app_server_root/scripts.wbm/crossCell** directory, but you can create your own properties file for your configuration:

     **configRemoteMonitorBus.sh -props** *properties_file_name*

     **configRemoteMonitorBus.bat -props** *properties_file_name*

   Where:

   *properties_file_name* is the fully qualified name of the properties file that contains the required values for the configuration. The path to the properties file must be fully specified for the script to find the properties file. The cross-cell configuration utility creates a service integration bus in the remote cell. The name of the bus is **MONITOR.<*remote_cell_name*>.bus**, where <*remote_cell_name*> is the name of the remote cell.

5. When the script completes, restart both the local IBM Business Monitor server and the remote CEI server.
6. Verify that the remote service integration bus exists and that the link between the local and remote buses was created successfully, by following the steps in the topic "Verifying the remote IBM Business Monitor bus and service integration link."

When you deploy a monitor model with a remote CEI, you need to select the **Remote** CEI location option, as described in the step entitled "Select Monitor model CEI options" in the topic Deploying monitor models.

**If you have a secured environment:** You can deploy a monitor model in a secured environment with a remote CEI and queue-based event management. After deploying a monitor model, you need to complete the installation by following the instructions in the topic "Completing the installation of a monitor model in a secured queue-based environment."

*Verifying the remote IBM Business Monitor bus and service integration link:*

After you have configured the IBM Business Monitor server to use the common event infrastructure (CEI) server on a remote WebSphere Application Server or Process Server, you must verify that you successfully created the remote bus and service integration link.

To verify that the remote bus and the service integration bus link exist and are active, complete the following steps:

1. From the administrative console on the remote WebSphere Application Server or Process Server, click **Service Integration** > **Buses**.
2. Click the **MONITOR.<*cell_name*>.bus** bus that you are verifying, where <*cell_name*> is the name of the cell where the remote CEI server is installed.
3. Under Topology, click **Messaging Engines**. One messaging engine is defined. The **Status** field displays a green arrow if the messaging engine is active.
4. Click the messaging engine, and then click **Additional Properties** > **Service integration bus links**. If you are connecting the remote cell to a single monitor installation and a monitor installation to a single remote cell, one link is defined. You can, however, have more than one link. The **Status** field displays a green arrow if the link is active.
5. Optional: To verify using the System.out log, look for a message similar to the following. The messaging engine name is different for each machine:

```
CWSIP0382I: Messaging engine FADB84EB685E209F responded to subscription request,
Publish Subscribe topology now consistent.
```

**Note:** You can perform the same procedure on the IBM Business Monitor server to validate that the IBM Business Monitor server side of the service integration bus link is active.

## Configuring Business Space

You can configure Business Space powered by WebSphere, which provides a common interface for application users to create, manage, and integrate web interfaces across the IBM Business Process Management portfolio, WebSphere Enterprise Service Bus, and other IBM products.

## Configuring Business Space

Install and configure Business Space powered by WebSphere to set up a common interface for application users to create, manage, and integrate web interfaces.

You must install the product software. When you install your product, Business Space files are included with the installation for the profiles that you configured.

Business Space is supported with the following database products:

- DB2 Universal
- DB2 for IBM i
- DB2 for z/OS
- Microsoft SQL Server
- Oracle 11g

To find out which databases are supported with the specific IBM product that you are using with Business Space, check the supported databases for the product.

If you install IBM Business Process Manager, WebSphere Enterprise Service Bus, or IBM Business Monitor and create a stand-alone server profile with the typical option, Business Space is installed and configured automatically with a DB2 Express database. If you are using a stand-alone server profile, you can use the Profile Management Tool with the advanced option to configure Business Space to work with your runtime environment. For more information, see "Configuring Business Space using the Profile Management Tool."

For all products, if you are setting up deployment manager and custom profiles, the simplest way to configure Business Space is with the Deployment Environment Configuration wizard. For more information, see "Configuring Business Space using the Deployment Environment Configuration wizard."

If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, Representational State Transfer (REST) service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST services. If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. You must register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.

If you are using deployment manager and custom profiles, you can use the administrative console to configure Business Space.

After your original setup work on the Profile Management Tool or the administrative console, you must also configure the database tables for Business Space. For more information, see "Configuring Business Space database tables."

No matter what tool you used to configure Business Space, you must make sure that Business Space works with the security for your environment. For more information, see "Setting up security for Business Space."

Business Space is built on IBM Mashup Center technology. For frequently asked questions and general troubleshooting information about IBM Mashup Center, see IBM Mashup Center Troubleshooting.

After you have installed and configured Business Space, users of your runtime environment can open it from the following URL: http://*host*:*port*/BusinessSpace, where *host* is the name of the host where your server is running and *port* is the port number for your server.

## Configuring Business Space on a product profile using the Profile Management Tool

You can configure Business Space powered by WebSphere as part of your product profile by using the Profile Management Tool.

You can start the Profile Management Tool after product installation. In addition, you can use the Profile Management Tool capabilities from the command line by using the **manageprofiles** command-line utility parameter **-configureBSpace** after product installation. In both situations, Business Space is installed with

the same database product as the database product you designate for the Common database. If you selected a database that is not supported with Business Space, the Profile Management Tool configures Business Space with the IBM DB2 Express database.

If you use the **manageprofiles** command-line utility, follow the **manageprofiles** documentation for your business process management product. Review the following considerations for using **manageprofiles**:

- If you use Oracle or SQL Server on a stand-alone server, you must create the database manually instead of using the **-dbCreateNew** parameter.
- If you have a remote database in a clustered environment, you must create the database manually, copy over the generated scripts to the remote machine with the database, and run the scripts from that location.

For deployment manager and custom profiles, you can use the administrative console or the Deployment Environment Configuration wizard. See "Configuring Business Space using the administrative console" or "Configuring Business Space using the Deployment Environment Configuration wizard". If you use the Profile Management Tool to create a deployment manager and custom profiles (managed nodes) with the **Deployment environment** profile creation option, Business Space is configured automatically with your deployment environment, but you must manually run scripts to configure the database tables.

For more advanced configuration options on a stand-alone server profile, you must use pages on the administrative console to configure Business Space. For example, if you want to designate a data source that is different than the database you selected for your profile (the IBM Business Monitor database or the IBM Business Process Manager common database), you must use the administrative console to configure Business Space.

If you have decided to use these more advanced configuration options, which require using the administrative console, make sure to complete the following steps:

- When you create the stand-alone server profile using the Profile Management Tool, use the **Advanced** profile creation option and clear the **Configure Business Space** check box, so you can configure Business Space later using the administrative console.
- See "Configuring Business Space using the administrative console."

Optionally, if you don't want to configure Business Space as part of your product profile, you can create separate Business Space profiles. You might want to separate the user interface on one machine and the back end on another machine for load separation. For example, you might want to put the IBM Business Process Manager server on one machine for the heavy workload, and put Business Space on a different remote machine to distribute the workload. The back-end machine can be tuned for back-end processing, and the Business Space machine can be set up to handle the HTTP traffic. For more information, see “Creating Business Space profiles” on page 144.

- For a stand-alone server, start the Profile Management Tool, select the **Stand-alone server profile** option and complete the following steps.
  1. Complete one of the following steps on the Profile Creation Options page:
     - Select the **Typical** profile creation option if you want to accept a default installation and configuration of Business Space using the DB2 Express database. (Skip steps b.-e.)
     - Select the **Advanced** option if you want to configure advanced options for the profile you are creating. Then on the Business Space Configuration page, make sure that the **Configure Business Space** check box is selected.

     Business Space is configured with your product data source.
  2. When you designate the host name for your profile, use a fully qualified host name.
  3. On the Database Design page, you have the option of using a database design file that you have created using the database design tool that contains all database configuration for your product, including the database configuration information for Business Space. For more information about database design files, see “Creating a Business Space database design properties file” on page 193.

4. Complete the profile creation using the Profile Management Tool. Business Space is installed. It is configured for the same database product that you designated for the Common database (or with DB2 Express if the database product is not supported).
5. If the database is remote, you must configure the database tables after running the Profile Management Tool. See "Configuring Business Space database tables."

- For a deployment environment, start the Profile Management Tool, select the **Deployment manager profile** or **Custom profile** option and complete the following steps.
  1. On the Profile Creation Options page, select the **Deployment environment** option to configure each profile with customized configuration values and use it in a deployment environment based on a supplied pattern.
  2. Follow the Profile Management Tool steps to create a deployment manager profile and custom profiles (managed nodes).
  3. After all the custom nodes are federated, run scripts to configure the database tables manually.

**Important:** If your product database is an Oracle database, Business Space is configured with the Profile Management Tool or the manageprofiles command-line utility to use the same database, with the default schema IBMBUSSP, and the default password that you enter during profile creation. If you want to use a different password for the IBMBUSSP user name, you must use the administrative console to update JDBC Resources:

1. Find the data source jdbc/mashupsDS.
2. Modify the value of the authentication alias to make it match the password of the Business Space schema name.
3. Save your changes and restart the server.

Before using Business Space, set up security that you need to use with Business Space and the widgets that your team is using. For more information, see "Setting up security for Business Space."

**Tip:** Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. For more information, see Changing the timeout settings for the Business Space Ajax proxy.

**Creating Business Space profiles:**

To create or augment Business Space profiles, you can use either the Profile Management Tool or the manageprofiles command-line utility. Profiles are sets of files that define the runtime environment for a deployment manager, a managed node, or a stand-alone server.

If Business Space is configured as part of your product profile, these tasks are optional.

*Creating Business Space profiles for a stand-alone configuration:*

To create Business Space profiles for a stand-alone environment, you can use either the Profile Management Tool or the manageprofiles command-line utility.

If Business Space is configured as part of your product profile, these tasks are optional.

*Creating Business Space profiles for a stand-alone configuration using the Profile Management Tool:*

Use the Profile Management Tool to create stand-alone profiles for Business Space.

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.

- When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons.
- If you plan to use a database design file for the Business Space database information, complete the steps in "Creating a Business Space database design properties file" on page 193.

Use this procedure if you are creating a Business Space profile for a stand-alone configuration. The steps describe both Advanced profile creation and Typical profile creation options.

If Business Space is configured as part of your product profile, this task is optional.

1. Start the Profile Management Tool.

   Use one of the following commands:

   - Linux UNIX *install_root*/bin/ProfileManagement/pmt.sh
   - Windows *install_root*\bin\ProfileManagement\pmt.bat

   The Welcome page opens.
2. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

   The Profiles tab opens.

   The Profiles tab contains a list of profiles that have been created on your machine. You can use the Profile Management Tool to create new profiles or augment existing profiles.
3. On the Profiles tab, click **Create**.

   The Environment Selection page opens in a separate window.
4. On the Environment Selection page, select the **Stand-alone profile** option and click **Next**.
5. On the Profile Creation Options page, decide whether to create the stand-alone profile using the **Typical profile creation** or **Advanced profile creation** option.
6. If you selected the **Typical profile creation** option, complete the following steps.
   a. On the Administrative Security page, enter values for the user name and password, confirm the password, and click **Next**.

      All profile configuration, including profile options and databases, are configured by default and displayed on the Profile Summary page.
   b. On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

      The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

      **Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

      - **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
      - **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

      The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.
7. If you selected the **Advanced profile creation** option, complete the following steps.
   a. On the Optional Application Deployment page, select the check boxes if you want to deploy the administrative console and the default application.
   b. On the Profile Name and Location page, perform the following steps:
      1) In the Profile name field, specify a unique name or accept the default value. Each profile that you create must have a name. When you have more than one profile, you can tell the profiles

apart at their highest level by this name. If you elect not to use the default name, for Windows, keep the name short, because path names are limited.

2) In the Profile directory field, type the directory for the profile or use the Browse button to go to the profile directory. The directory that you specify contains the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on your operating system:

   - Linux UNIX *install_root*/**profiles**/*profile_name*
   - Windows *install_root***profiles***profile_name*

     where *profile_name* is the name you specified.

   The profile directory field must meet the following requirements:

   - The *profile_name* must be unique.
   - The directory you specify must be empty.
   - Your user ID must have permissions for the directory.
   - There must be sufficient space to create the profile.

3) Optional: Select the **Make this profile the default** check box if you want to make the profile you are creating the default profile. This check box appears only if you have an existing profile on your system.

   Commands work automatically with the default profile. The first profile that you create on a workstation is the default profile. The default profile is the default target for commands that are issued from the bin directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies.

4) Click **Next**.

c. On the Node and Host Names page, perform the following actions for the profile you are creating:

   - In the Node name field, enter a name for the node or accept the default value. Keep the node name as short as possible, but ensure that node names are unique within your deployment environment.
   - In the Host name field, enter a name for the host or accept the default value.
   - In the Cell name field, enter a name for the cell or accept the default value.

   Click **Next** to display the Administrative Security page.

d. On the Administrative Security page, enter values for the user name and password and confirm the password. Click **Next**.

e. On the Security Certificate (Part 1) page, specify whether to create new certificates or import existing certificates. Perform the following actions:

   - To create a new default personal certificate and a new root signing certificate, select **Create a new default personal certificate** and **Create a new root signing certificate** and click **Next**.
   - To import existing certificates, select **Import an existing default personal certificate** and **Import an existing root signing personal certificate** and provide the following information:
     - In the Path field, enter the directory path to the existing certificate.
     - In the Password field, type the password for the certificate.
     - In the Keystore type field, select the keystore type for the certificate that you are importing.
     - In the Keystore alias field, select the keystore alias for the certificate that you are importing.
     - Click **Next**.

   When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

f. On the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next** to display the Port Values Assignment page.

   If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

   When you create either or both certificates, or import either or both certificates, the following keystore files are created:

   - `key.p12`: Contains the default personal certificate.
   - `trust.p12`: Contains the signer certificate from the default root certificate.
   - `root-key.p12`: Contains the root signing certificate.
   - `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower® signer certificate are in this keystore file.
   - `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
   - `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

   These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. An imported certificate is added to the `key.p12` file or the `root-key.p12` file. If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

g. On the Port Values Assignment page, verify that the ports specified for the profile are unique and click **Next**.

   The Profile Management Tool detects ports currently used by other IBM WebSphere products and displays recommended port values that do not conflict with existing ones. If you have other applications that use specified ports, verify that the ports do not conflict. If you chose not to deploy the administrative console on the Optional Application Deployment page, the administrative console ports are not available on the Port Values Assignment page. Ports are recognized as being in use if they are assigned to a profile created under an installation performed by the current user, or if they are currently in use.

   Although the tool validates ports when you access the Port Values Assignment page, port conflicts might result from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes. If you suspect a port conflict, you can investigate it after the profile is created.

   Determine the ports used during profile creation by examining the `profile_root/properties/portdef.props` file. Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in existing profiles in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the `ws_ant` script detailed in the topic.

h. If you are installing on a Linux or Windows platform, and have root or administrator group privileges, the Linux or Windows Service Definition page is displayed. On the Service Definition page, indicate whether the process server will run on a Windows service or Linux service and click **Next** to display the Web Server Definition page.

   Windows The Windows Service Definition page opens for the Windows platform only when the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the

**startServer** or **startManager** commands. For example, if you configure a server or deployment manager as a Windows service and issue the **startServer** or **startManager** commands, the **wasservice** command starts the defined services.

**Important:** If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is Manual). The user ID must not have spaces in the name, it must belong to the Administrator group, and it must have the advanced user right: Log on as a service. If the user ID belongs to the Administrator group, the Profile Management Tool grants the ID the advanced user right if it does not already have it. During profile deletion, you can remove the Windows service that is added during profile creation.

Windows **IPv6 considerations when running profiles as Windows services:** Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

Linux The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions. Your product attempts to start Linux services for processes that are started by the **startServer** or **startManager** commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or **startManager** commands, the **wasservice** command starts the defined services. By default, your product is not selected to run as a Linux service. To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a nonroot user ID, the Linux Service Definition page is not displayed, and no service is created. You must specify a user name under which the service runs. To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

i. If you are installing on any other operating system, or as a nonroot user on a Linux operating system or a nonadministrative user on a Windows operating system, the Web Server Definition page is displayed. To include a web server definition in the profile now, perform the following steps:
   1) Select the **Create a Web server definition** check box.
   2) Specify the web server characteristics on the page, and click **Next**.
   3) Specify the web server characteristics on Part 2 of the page.

      If you use a web server to route requests to your server, you need to include a web server definition. You can include the definition now, or define the web server to Business Space later. If you define the web server definition during the creation of this profile, you can install the web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the web Server Definition pages. If you define the web server to Business Space after you create this profile, you must define the web server in a separate profile.
   4) Click **Next**.

j. If you want to use a database design file that you have already created to configure the databases, complete the following steps instead of using the Database Configuration pages.
   1) Select **Use a database design file** for database configuration.
   2) Click **Browse**.

3) Specify the fully qualified path name for the design file.
4) Click **Next**.

k. If you haven't used a database design file, on the Database Configuration page, perform the following actions:
1) From the **Select a database** product list, select the database product to be used by the profile.
2) Select the **Override the default output directory for database scripts** check box if you want to set the directory into which the sql scripts used to create the database tables are written. If you do not select the check box, the scripts are output to the default directory.
3) Click **Next** to display the Database Configuration (Part 2) page.

The information on the Database Configuration (Part 2) page varies depending on the value specified from the Select a database product list on the Database Configuration page.

l. On the Database Configuration (Part 2) page, complete the database configuration. Depending on your database product, you must specify a user name and password to authenticate with the database, the JDBC driver information, and host, port, and schema.

m. On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

**Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

- **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
- **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

*Creating Business Space profiles for a stand-alone configuration using the manageprofiles command-line utility:*

You can use the manageprofiles command-line utility to create Business Space profiles for your Business Space stand-alone server configuration.

Before you run the manageprofiles command-line utility, make sure that you have completed the following tasks:

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- Review example profile creation commands.
- Verify that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.

This task describes how to use the manageprofiles command-line utility to create Business Space profiles for your Business Space stand-alone configuration. To use the manageprofiles command-line utility to create a profile, perform the following steps.

1. Locate the default.bspace profile template for Business Space stand-alone profiles, which define stand-alone servers.

   Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.
2. Determine which parameters are required for creating the profile by reviewing the "manageprofiles command-line utility (for Business Space profiles)" on page 169 topic. Determine the values that you

want to supply for the profile by reviewing the default values to see if they are what you need for your profile. For example, you might use the -templatePath, -enableAdminSecurity, -adminUserName, -adminPassword, -dbType, -dbUserId, -dbPassword, -dbJDBCClasspath, -dbName, -bspaceSchema, -dbHostName, -dbServerPort, and -dbDelayConfig parameters.

If you are using Windows Authentication with Microsoft SQL Server, make sure to specify the **-dbWinAuth** parameter as **true**.

3. Run the file from the command line. Here is a simple example:

```
manageProfiles -create -templatePath install_root/profileTemplates/BusinessSpace/default.bspace
 -enableAdminSecurity true -adminUserName admin_user_name -adminPassword admin_password
 -dbType DB2_DataServer -dbUserId db2_user_id -dbPassword db2_user_password
 -dbJDBCClasspath install_root/jdbcdrivers/DB2 -dbName database_name -bspaceSchema
 database_schema_name -dbHostName host_name -dbServerPort port_number -dbDelayConfig false
```

The command displays status as it runs. Wait for it to finish. Normal syntax checking on the response file applies as the file is parsed like any other response file. Individual values in the response file are treated as command-line parameters.

*Creating Business Space profiles for a network deployment configuration:*

To create Business Space profiles for a network deployment environment, you can use either the Profile Management Tool or the manageprofiles command-line utility.

If Business Space is configured as part of your product profile, these tasks are optional.

*Creating Business Space profiles for a network deployment configuration using the Profile Management Tool:*

You can use the Profile Management Tool to create Business Space profiles for a network deployment configuration: you create a deployment manager profile and custom profiles (managed nodes).

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons.

Use this procedure if you are creating a Business Space profile for a network deployment configuration. You create a deployment manager profile and custom profiles for managed nodes. The steps describe both Advanced profile creation and Typical profile creation options.

If Business Space is configured as part of your product profile, this task is optional.

1. Create the deployment manager profile.
   a. Start the Profile Management Tool.

      Use one of the following commands:

      - Linux UNIX ***install_root*/bin/ProfileManagement/pmt.sh**
      - Windows ***install_root*\bin\ProfileManagement\pmt.bat**

   b. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

      The Profiles tab opens.

      The Profiles tab contains a list of profiles that have been created on your machine. You can use the Profile Management Tool to create new profiles or augment existing profiles.

   c. On the Profiles tab, click **Create**.

      The Environment Selection page opens in a separate window.

d. On the Environment Selection page, expand the **Business Space powered by WebSphere** section, select the **Business Space powered by WebSphere deployment manager** option and click **Next**.

e. On the Profile Creation Options page, decide whether to create the stand-alone profile using the **Typical profile creation** or **Advanced profile creation** option.

f. If you selected the **Typical profile creation** option, complete the following steps.

1) On the Administrative Security page, enter values for the user name and password, confirm the password, and click **Next**. All profile configuration, including profile options and databases, are configured by default and displayed on the Profile Summary page.

2) On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

**Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

- **The Profile Management tool created the profile but errors occurred**
- **The Profile Management tool cannot create the profile**

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

g. If you selected the **Advanced profile creation** option, complete the following steps.

1) On the Optional Application Deployment page, select the check boxes if you want to deploy the administrative console and the default application.

2) On the Profile Name and Location page, perform the following steps:

a) In the Profile name field, specify a unique name or accept the default value. Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name. If you elect not to use the default name, for Windows, keep the name short, because path names are limited.

b) In the Profile directory field, type the directory for the profile or use the Browse button to go to the profile directory. The directory that you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on the operating system that you are using:

- Linux UNIX *install_root*/**profiles**/*profile_name*
- Windows *install_root***profiles***profile_name*

where *profile_name* is the name you specified.

The profile directory field must meet the following requirements:

- The *profile_name* must be unique.
- The directory you specify must be empty.
- Your user ID must have permissions for the directory.
- There must be sufficient space to create the profile.

c) Optional: Select the **Make this profile the default** check box if you want to make the profile you are creating the default profile. This check box appears only if you have an existing profile on your system.

Commands work automatically with the default profile. The first profile that you create on a workstation is the default profile. The default profile is the default target for commands that are issued from the bin directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies.

d) Click **Next**.

3) On the Node and Host Names page, perform the following actions for the profile you are creating:
   a) In the Node name field, enter a name for the node or accept the default value. Keep the node name as short as possible, but ensure that node names are unique within your deployment environment.
   b) In the Host name field, enter a name for the host or accept the default value.
   c) In the Cell name field, enter a name for the cell or accept the default value.

   Click **Next** to display the Administrative Security page.
4) On the Administrative Security page, enter values for the user name and password and confirm the password. Click **Next**.
5) On the Security Certificate (Part 1) page, specify whether to create new certificates or import existing certificates. Perform the following actions:
   - To create a new default personal certificate and a new root signing certificate, select **Create a new default personal certificate** and **Create a new root signing certificate** and click **Next**.
   - To import existing certificates, select **Import an existing default personal certificate** and **Import an existing root signing personal certificate** and provide the following information:
     – In the Path field, enter the directory path to the existing certificate.
     – In the Password field, type the password for the certificate.
     – In the Keystore type field, select the keystore type for the certificate that you are importing.
     – In the Keystore alias field, select the keystore alias for the certificate that you are importing.
     – Click **Next**.

     When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.
6) On the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next** to display the Port Values Assignment page.

   If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

   When you create either or both certificates, or import either or both certificates, the following keystore files are created:
   - `key.p12`: Contains the default personal certificate.
   - `trust.p12`: Contains the signer certificate from the default root certificate.
   - `root-key.p12`: Contains the root signing certificate.
   - `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
   - `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
   - `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. An imported certificate is added to the `key.p12` file or the `root-key.p12` file. If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

7) On the Port Values Assignment page, verify that the ports specified for the profile are unique and click **Next**.

   The Profile Management Tool detects ports currently used by other IBM WebSphere products and displays recommended port values that do not conflict with existing ones. If you have other applications that use specified ports, verify that the ports do not conflict. If you chose not to deploy the administrative console on the Optional Application Deployment page, the administrative console ports are not available on the Port Values Assignment page. Ports are recognized as being in use if they are assigned to a profile created under an installation performed by the current user, or if they are currently in use.

   Although the tool validates ports when you access the Port Values Assignment page, port conflicts might result from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes. If you suspect a port conflict, you can investigate it after the profile is created.

   Determine the ports used during profile creation by examining the `profile_root/properties/portdef.props` file. Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in existing profiles in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the `ws_ant` script detailed in the topic.

8) If you are installing on a Linux or Windows platform, and have root or Administrator group privileges, the Linux or Windows Service Definition page is displayed. On the Service Definition page, indicate whether a Windows service or Linux service will run the process server and click **Next** to display the Web Server Definition page.

   Windows The Windows Service Definition page opens for the Windows platform only when the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Windows service and issue the startServer or startManager commands, the wasservice command starts the defined services.

   **Important:** If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is Manual). The user ID must not have spaces in the name, it must belong to the Administrator group, and it must have the advanced user right: Log on as a service. If the user ID belongs to the Administrator group, the Profile Management Tool grants the ID the advanced user right if it does not already have it. During profile deletion, you can remove the Windows service that is added during profile creation.

   Windows **IPv6 considerations when running profiles as Windows services:** Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

Linux The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions. Your product attempts to start Linux services for processes that are started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or startManager commands, the wasservice command starts the defined services. By default, your product is not selected to run as a Linux service. To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, the Linux Service Definition page is not displayed, and no service is created. You must specify a user name under which the service runs. To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

9) On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

**Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

- **The Profile Management tool created the profile but errors occurred**
- **The Profile Management tool cannot create the profile**

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

2. Start the deployment manager profile.

Start the deployment manager using the **startServer** command from the *profile_root*/bin directory. Use the following syntax:

- Linux UNIX **startServer.sh** *server_name*
- Windows **startServer.bat** *server_name*

For more information about the **startServer** command, see the startServer command topic on the WebSphere Application Server, Version 8.0 information center.

3. Create the custom profiles (managed nodes).

a. Start the Profile Management Tool.

Use one of the following commands:

- Linux UNIX *install_root*/**bin/ProfileManagement/pmt.sh**
- Windows *install_root***bin\ProfileManagement\pmt.bat**

b. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

The Profiles tab opens.

The Profiles tab contains a list of profiles that have been created on your machine. You can use the Profile Management Tool to create new profiles or augment existing profiles.

c. On the Profiles tab, click **Create**.

The Environment Selection page opens in a separate window.

d. On the Environment Selection page, expand the **Business Space powered by WebSphere** section, select the **Business Space powered by WebSphere custom profile** option and click **Next**.

e. On the Profile Creation Options page, decide whether to create the stand-alone profile using the **Typical profile creation** or **Advanced profile creation** option.

f. If you selected the **Typical profile creation** option, complete the following steps.

1) On the Federation page, choose to federate the node into the deployment manager now as part of the profile creation, or at a later time with the addNode command apart from profile creation. Select or clear the **Federate this node later** check box, and click **Next**.
2) On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

   The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   **Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

   - **The Profile Management tool created the profile but errors occurred**
   - **The Profile Management tool cannot create the profile**

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

g. If you selected the **Advanced profile creation** option, complete the following steps.
1) On the Profile Name and Location page, perform the following steps:
   a) In the Profile name field, specify a unique name or accept the default value. Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name. If you elect not to use the default name, for Windows, keep the name short, because path names are limited.
   b) In the Profile directory field, type the directory for the profile or use the Browse button to go to the profile directory. The directory that you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on platform:

      - Linux UNIX ***install_root*/profiles/*profile_name***
      - Windows ***install_root*\profiles*profile_name***

        where *profile_name* is the name you specified.

      The profile directory field must meet the following requirements:

      - The *profile_name* must be unique.
      - The directory you specify must be empty.
      - Your user ID must have permissions for the directory.
      - There must be sufficient space to create the profile.

   c) Optional: Select the **Make this profile the default** check box if you want to make the profile you are creating the default profile. This check box appears only if you have an existing profile on your system.

      Commands work automatically with the default profile. The first profile that you create on a workstation is the default profile. The default profile is the default target for commands that are issued from the bin directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies.
   d) Click **Next**.
2) On the Node and Host Names page, perform the following actions for the profile you are creating:
   a) In the Node name field, enter a name for the node or accept the default value. Keep the node name as short as possible, but ensure that node names are unique within your deployment environment.
   b) In the Host name field, enter a name for the host or accept the default value.

c) In the Cell name field, enter a name for the cell or accept the default value.

Click **Next** to display the Administrative Security page.

3) On the Federation page, choose to federate the node into the deployment manager now as part of the profile creation, or at a later time with the addNode command apart from profile creation. Select or clear the **Federate this node later** check box, and click **Next**.

4) On the Security Certificate (Part 1) page, specify whether to create new certificates or import existing certificates. Perform the following actions:

   - To create a new default personal certificate and a new root signing certificate, select **Create a new default personal certificate** and **Create a new root signing certificate** and click **Next**.
   - To import existing certificates, select **Import an existing default personal certificate** and **Import an existing root signing personal certificate** and provide the following information:
     – In the Path field, enter the directory path to the existing certificate.
     – In the Password field, type the password for the certificate.
     – In the Keystore type field, select the keystore type for the certificate that you are importing.
     – In the Keystore alias field, select the keystore alias for the certificate that you are importing.
     – Click **Next**.

   When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

5) On the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next** to display the Port Values Assignment page.

   If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

   When you create either or both certificates, or import either or both certificates, the following keystore files are created:

   - `key.p12`: Contains the default personal certificate.
   - `trust.p12`: Contains the signer certificate from the default root certificate.
   - `root-key.p12`: Contains the root signing certificate.
   - `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
   - `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
   - `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

   These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. An imported certificate is added to the `key.p12` file or the `root-key.p12` file. If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

6) On the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

**Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

- **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
- **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

4. Log on to the deployment manager administrative console.
5. Depending on whether you want to deploy Business Space to a cluster or to managed servers, perform one of the following actions:
   - For a cluster:
     a. Create an application server cluster.
     b. Add one or more cluster members to the cluster (these are the Business Space custom profiles that were previously created).
   - For each managed server:
     a. Create an application server.
     b. Select the managed server's node to be the Business Space custom profile that was previously created.
6. Stop the deployment manager profile.

   Stop the deployment manager using the **stopServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **stopServer.sh** *server_name* **-username** *user_name* **-password** *password*
   - Windows **stopServer.bat** *server_name* **-username** *user_name* **-password** *password*

   If the profile does not have security enabled the **-username** and **-password** parameters are not necessary.

   For more information about the **stopServer** command, see the stopServer command topic on the WebSphere Application Server, Version 8.0 information center.
7. Navigate to the *install_root*/BusinessSpace/config.bspace/MetadataFiles directory and depending on the database type that you will be using for Business Space, copy the relevant file to a working directory. Do not change the extension of this file: it must be .properties.
   a. Edit the copy of this file and modify the values to correspond to your database. Make sure that the **wasHome** property is correct.
   b. When you have completed editing this file with your database information, save it.

After you have created the profiles and configured the database information for your profiles, you can configure Business Space in your environment by completing the following steps.

1. For each cluster or managed server run the **installBusinessSpace** command to install the Business Space enterprise archive (EAR) files in your runtime environment. Provide either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. See "Configuring Business Space using the command line" on page 191.
2. For each cluster or managed server, run the **configureBusinessSpace** command providing either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. Also specify the **bspacedbDesign** parameter. The value for this parameter should be the path to the database properties file that you previously edited. Optionally, if

you want to create database tables and configure the Business Space database, specify the **createTables** parameter as true. See "Configuring Business Space using the command line" on page 191.

3. Save the wsadmin configuration.
4. If the **createTables** parameter was not specified in step 2, create and configure the Business Space database. See "Configuring the Business Space database" on page 193.
5. Start the deployment manager.
6. Start the clusters or managed servers.

*Creating the Business Space profiles for a network deployment configuration using the manageprofiles command-line utility:*

You can use the manageprofiles command-line utility to create deployment manager profiles and custom profiles (managed nodes) for your Business Space network deployment configuration.

Before you run the manageprofiles command-line utility, make sure that you have completed the following tasks:

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- Review example profile creation commands.
- Verify that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.

This task describes how to use the manageprofiles command-line utility to create Business Space profiles for your Business Space network deployment configuration. To use the manageprofiles command-line utility to create a profile, perform the following steps.

1. Create the deployment manager profile.
   a. Locate the dmgr.bspace template for Business Space deployment manager profiles, which define deployment managers. A deployment manager provides one administrative interface to a logical group of servers on one or more workstations.

      Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.
   b. Determine which parameters are required for creating the profile by reviewing the "manageprofiles command-line utility (for Business Space profiles)" on page 169 topic. Determine the values that you want to supply for the profile by reviewing the default values to see if they are what you need for your profile. For example, you might include the -templatePath, -serverType, -enableAdminSecurity, -adminUserName, and -adminPassword parameters.
   c. Run the file from the command line. Here is a simple example:

      ```
      manageProfiles -create -templatePath install_root/profileTemplates/BusinessSpace/dmgr.bspace
       -serverType DEPLOYMENT_MANAGER -enableAdminSecurity true -adminUserName admin_user_ID
      -adminPassword admin_password
      ```

      The command displays status as it runs. Wait for it to finish. Normal syntax checking on the response file applies as the file is parsed like any other response file. Individual values in the response file are treated as command-line parameters.
2. Start the deployment manager profile.

   Start the deployment manager using the **startServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **startServer.sh** *server_name*
   - Windows **startServer.bat** *server_name*

For more information about the **startServer** command, see the startServer command topic on the WebSphere Application Server, Version 8.0 information center.

3. Create the custom profiles (managed nodes).
   a. Locate the managed.bspace template for Business Space custom profiles, which, when federated to a deployment manager, define managed nodes. If you have decided that your solution requires a deployment environment, your runtime environment requires one or more managed nodes. A custom profile contains an empty node that you must federate into a deployment manager cell to make operational. Federating the custom profile changes it into a managed node. Do not federate a node unless the deployment manager you are federating to is at a release level the same or higher than that of the custom profile you are creating.

      Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.
   b. Determine which parameters are required for creating the profile by reviewing the "manageprofiles command-line utility (for Business Space profiles)" on page 169 topic. Determine the values that you want to supply for the profile by reviewing the default values to see if they are what you need for your profile. For example, you might include the -templatePath, -dmgrAdminUserName, -dmgrAdminPassword, -dmgrPort, and -dmgrHost parameters.
   c. Run the file from the command line. Here is a simple example:

      ```
      manageProfiles -create -templatePath install_root/profileTemplates/BusinessSpace/managed.bspace
      -dmgrAdminUserName deployment_manager_admin_user_ID
      -dmgrAdminPassword deployment_manager_admin_password -dmgrPort deployment_manager_port
      -dmgrHost deployment_manager_host_name
      ```

      The command displays status as it runs. Wait for it to finish. Normal syntax checking on the response file applies as the file is parsed like any other response file. Individual values in the response file are treated as command-line parameters.
4. Log on to the deployment manager administrative console.
5. Depending on whether you want to deploy Business Space to a cluster or to managed servers, create one of the following:
   - For a cluster:
     a. Create an application server cluster.
     b. Add one or more cluster members to the cluster (these are the Business Space custom profiles that were previously created).
   - For each managed server:
     a. Create an application server.
     b. Select the managed server's node to be the Business Space custom profile that was previously created.
6. Stop the deployment manager profile.

   Stop the deployment manager using the **stopServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **stopServer.sh** *server_name* **-username** *user_name* **-password** *password*
   - Windows **stopServer.bat** *server_name* **-username** *user_name* **-password** *password*

   If the profile does not have security enabled the **-username** and **-password** parameters are not necessary.

   For more information about the **stopServer** command, see the stopServer command topic on the WebSphere Application Server, Version 8.0 information center.
7. Navigate to the *install_root*/BusinessSpace/config.bspace/MetadataFiles directory and depending on the database type that you will be using for Business Space, copy the relevant file to a working directory. Do not change the extension of this file: it must be .properties.

a. Edit the copy of this file and modify the values to correspond to your database. Pay special attention to property **wasHome** and make sure that it is correct.
b. When you have completed editing this file with your database information, save it.

After you have created the profiles and configured the database information for your profiles, you can configure Business Space in your environment by completing the following steps.

1. For each cluster or managed server run the **installBusinessSpace** command to install the Business Space enterprise archive (EAR) files in your runtime environment. Provide either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. See "Configuring Business Space using the command line" on page 191.
2. For each cluster or managed server, run the **configureBusinessSpace** command providing either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. Also specify the **bspacedbDesign** parameter. The value for this parameter should be the path to the database properties file that you previously edited. Optionally, if you want to create database tables and configure the Business Space database, specify the **createTables** parameter as true. See "Configuring Business Space using the command line" on page 191.
3. Save the wsadmin configuration.
4. If the **createTables** parameter was not specified in step 2, create and configure the Business Space database. See "Configuring the Business Space database" on page 193.
5. Start the deployment manager.
6. Start the clusters or managed servers.

*Augmenting Business Space profiles for a stand-alone configuration:*

To augment Business Space profiles for a stand-alone environment, you can use either the Profile Management Tool or the manageprofiles command-line utility.

If Business Space is configured as part of your product profile, these tasks are optional.

*Augmenting Business Space profiles for a stand-alone configuration using the Profile Management Tool:*

You can use the Profile Management Tool to augment stand-alone profiles for Business Space.

Understand the concepts of profiles, including the differences between stand-alone, network deployment and custom profiles. Understand the differences between the Typical profile augmentation option and the Advanced profile augmentation option, including under which scenarios you should use one over the other. The Typical profile augmentation option augments a profile with default configuration settings. The Advanced profile augmentation option lets you specify your own configuration values for the profile you are augmenting.

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons.
- If you plan to use a database design file for the Business Space database information, complete the steps in "Creating a Business Space database design properties file" on page 193.

Use this procedure if you are augmenting a Business Space profile for a stand-alone configuration. The steps describe both Advanced profile creation and Typical profile creation options.

If Business Space is augmented as part of your product profile, this task is optional.

1. Start the Profile Management Tool.

Use one of the following commands:

- Linux UNIX *install_root*/bin/ProfileManagement/pmt.sh
- Windows *install_root*\bin\ProfileManagement\pmt.bat

The Welcome page opens.

2. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

   The Profiles tab opens.

   The Profiles tab contains a list of profiles on your machine currently. For this procedure, it is assumed you are augmenting an existing application server profile with Business Space in a stand-alone configuration.

3. Select the profile that you want to augment, and click **Augment**. The **Augment** button cannot be selected unless a profile can be augmented.

   The Augment Selection page opens in a separate window.

4. On the Augment Selection page, if the profile can be augmented to Business Space, the **Stand-alone profile** option is available. Click **Next**.

5. On the Profile Augmentation Option page, decide whether to augment the stand-alone profile using the **Typical profile augmentation** or **Advanced profile augmentation** option.

   The Typical profile augmentation option augments a profile with default configuration settings. The Advanced profile augmentation option lets you specify your own configuration values for the profile you are augmenting.

6. If you selected the **Typical profile augmentation** option, complete the following steps.

   a. On the Administrative Security page, re-enter the administrative user ID and password for the profile you are augmenting.

   b. On the Profile Augmentation Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

      The progress of the augmentation is displayed in the Profile Configuration Progress window. When the profile augmentation is complete, the Profile Augmentation Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

      **Attention:** If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

      - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
      - **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

      The Profile Augmentation Complete page identifies the log file to reference in order to troubleshoot the problems.

7. If you selected the **Advanced profile augmentation** option, complete the following steps.

   a. On the Administrative Security page, re-enter the administrative user ID and password for the profile you are augmenting.

   b. If you want to use a design file that you have already created to configure the databases for the augmented profile, complete the following steps instead of using the Database Configuration pages.

      1) Select **Use a database design file** for database configuration.
      2) Click **Browse**.
      3) Specify the fully qualified path name for the design file.
      4) Click **Next**.

c. If you haven't used a database design file, on the Database Configuration page, perform the following actions:
   1) From the Select a database product list, select the database product to be used by the profile.
   2) Select the **Override the default output directory for database scripts** check box if you want to set the directory into which the sql scripts used to create the database tables are written. If you do not select the check box, the scripts are output to the default directory.
   3) Click **Next** to display the Database Configuration (Part 2) page.

   The information on the Database Configuration (Part 2) page varies depending on the value specified from the Select a database product list on the Database Configuration page.
d. On the Database Configuration (Part 2) page, complete the database configuration. Depending on your database product, you must specify a user name and password to authenticate with the database, the JDBC driver information, and host, port, and schema.
e. On the Profile Augmentation Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

   The progress of the augmentation is displayed in the Profile Configuration Progress window. When the profile augmentation is complete, the Profile Augmentation Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

   **Attention:** If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:
   - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
   - **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

   The Profile Augmentation Complete page identifies the log file to reference in order to troubleshoot the problems.

If you augment to a profile that already has security set up with a user repository that is not the default federated repositories option, you must check the `ConfigServices.properties` file to adjust the MashupAdminForOOBSpace parameter. See “Selecting the user repository for Business Space” on page 216.

*Augmenting Business Space profiles for a stand-alone configuration using the manageprofiles command-line utility:*

You can augment stand-alone profiles for Business Space from the command line using the manageprofiles command-line utility.

Before you run the **manageprofiles** command-line utility to augment a profile, make sure that you have completed the following tasks:
- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- Review example profile creation commands.
- Verify that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.
- Shut down any servers associated with the profile that you plan to augment.
- Determine if the profile you plan to augment has already been federated to a deployment manager. If the profile you want to augment has already been federated to a deployment manager, you cannot augment it using the manageprofiles command-line utility.
- Determine the template that the existing profile was created with (deployment manager, stand-alone, or managed). You can determine the template that was used for creating the profile by viewing the profile

registry in *install_root*/properties/profileRegistry.xml. Do not modify this file, use it only to view the templates. For this procedure it is assumed that you are augmenting a Process Server stand-alone profile.

To use the **manageprofiles** command-line utility to augment a Business Space profile for a stand-alone configuration, perform the following steps.

If Business Space is augmented as part of your product profile, this task is optional.

1. Locate the default.bspace profile template for Business Space stand-alone profiles, which define stand-alone servers.

   Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.

   You use the **augment** parameter to make changes to an existing profile with an augmentation template. The **augment** parameter causes the **manageprofiles** command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment. Make sure that you specify the fully qualified file path for **-templatePath**, because a relative file path results in the specified profile not being fully augmented.
2. Run the file from the command line. Do not supply a **-profilePath** parameter. Here is a simple example:

   ```
   manageProfiles -augment -profileName profile_name -templatePath
    install_root/profileTemplates/BusinessSpace/default.bspace -cellName cell_name
    -nodeName node_name -enableAdminSecurity true -adminUserName admin
    -adminPassword admin -dbType DB2_DataServer -dbUserId database_user_ID
    -dbPassword database_password -dbJDBCClasspath install_root/jdbcdrivers/DB2
    -dbName database_name -bspaceSchema database_schema -dbHostName
    database_host_name -dbServerPort database_port -dbDelayConfig false
   ```

   The **-cellName** and **-nodeName** parameters are optional. If you don't specify the **-cellName** and **-nodeName** parameters, the default is the existing profile you are using.

   The status is written to the console window when the command is finished running.

If you augment to a profile that already has security set up with a user repository that is not the default federated repositories option, you must check the ConfigServices.properties file to adjust the MashupAdminForOOBSpace parameter. See “Selecting the user repository for Business Space” on page 216.

*Augmenting Business Space profiles for a network deployment configuration:*

To augment Business Space profiles for a network deployment configuration, you can use either the Profile Management Tool or the manageprofiles command-line utility.

If Business Space is configured as part of your product profile, these tasks are optional.

*Augmenting Business Space profiles for a network deployment configuration using the Profile Management Tool:*

You can use the Profile Management Tool to augment Business Space profiles for a network deployment environment.

Understand the concepts of profiles, including the differences between stand-alone, network deployment and custom profiles. Understand the differences between the Typical profile augmentation option and the Advanced profile augmentation option, including under which scenarios you should use one over the other. The Typical profile augmentation option augments a profile with default configuration settings. The Advanced profile augmentation option lets you specify your own configuration values for the profile you are augmenting.

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.

- When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons.

Use this procedure if you are augmenting a Business Space profile for a network deployment configuration. The steps describe both Advanced profile creation and Typical profile augmentation options. This procedure assumes that you have an existing deployment manager profile and custom profiles (managed nodes) that you want to augment to Business Space.

If Business Space is augmented as part of your product profile, this task is optional.

1. Augment the deployment manager profile.
   a. Start the Profile Management Tool.

      Use one of the following commands:

      - Linux UNIX *install_root*/bin/ProfileManagement/pmt.sh
      - Windows *install_root*\bin\ProfileManagement\pmt.bat

   b. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

      The Profiles tab opens.

      The Profiles tab contains a list of profiles that have been created on your machine. You can use the Profile Management Tool to create new profiles or augment existing profiles.

   c. On the Profiles tab, click **Augment**.

      The Augment Selection page opens in a separate window.

   d. On the Augment Selection page, expand the **Business Space powered by WebSphere** section, select the **Business Space deployment manager** option and click **Next**.

   e. On the Profile Augmentation Options page, decide whether to augment the stand-alone profile using the **Typical profile augmentation** or **Advanced profile augmentation** option.

   f. On the Administrative Security page, enter values for the user name and password, confirm the password, and click **Next**. All profile configuration, including profile options, are configured by default and displayed on the Profile Augmentation Summary page.

   g. On the Profile Augmentation Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

      The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Augmentation Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

      **Attention:** If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

      - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
      - **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

      The Profile Augmentation Complete page identifies the log file to reference in order to troubleshoot the problems.

2. Start the profile.

   Start the profile using the **startServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **startServer.sh** *server_name*
   - Windows **startServer.bat** *server_name*

For more information about the **startServer** command, see the startServer command topic on the WebSphere Application Server, Version 8.0 information center.

3. Augment the custom profiles (managed nodes).
   a. Start the Profile Management Tool.

      Use one of the following commands:

      - Linux UNIX *install_root*/bin/ProfileManagement/pmt.sh
      - Windows *install_root*\bin\ProfileManagement\pmt.bat

   b. On the Welcome page, click **Launch Profile Management Tool** or select the Profile Management Tool tab.

      The Profiles tab opens.

      The Profiles tab contains a list of profiles that have been created on your machine. You can use the Profile Management Tool to create new profiles or augment existing profiles.

   c. On the Profiles tab, click **Augment**.

      The Augment Selection page opens in a separate window.

   d. On the Augment Selection page, expand the **Business Space powered by WebSphere** section, select the **Business Space custom profile** option and click **Next**.

   e. On the Profile Augmentation Options page, decide whether to create the stand-alone profile using the **Typical profile creation** or **Advanced profile creation** option.

   f. On the Federation page, choose to federate the node into the deployment manager now as part of the profile creation, or at a later time with the addNode command apart from profile creation. Select or clear the **Federate this node later** check box, and click **Next**.

   g. On the Profile Augmentation Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

      The progress of the configuration is displayed in the Profile Configuration Progress window. When the profile creation is complete, the Profile Augmentation Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

      **Attention:** If errors are detected during profile creation, other messages might appear in place of the success message, for example:

      - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
      - **The Profile Management tool cannot augment the profile**, which indicates that profile creation failed completely.

      The Profile Augmentation Complete page identifies the log file to reference in order to troubleshoot the problems.

4. Log on to the deployment manager administrative console.
5. Optional: If you don't already have a cluster or managed servers, do one of the following for your environment:
   - For a cluster:
     a. Create an application server cluster.
     b. Add one or more cluster members to the cluster (these are the Business Space custom profiles that were previously created).
   - For each managed server:
     a. Create an application server.
     b. Select the managed server's node to be the Business Space custom profile that was previously created.
6. Stop the deployment manager profile.

   Stop the deployment manager using the **stopServer** command from the *profile_root*/bin directory.

Use the following syntax:

- Linux UNIX **stopServer.sh** *server_name* **-username** *user_name* **-password** *password*
- Windows **stopServer.bat** *server_name* **-username** *user_name* **-password** *password*

If the profile does not have security enabled the **-username** and **-password** parameters are not necessary.

For more information about the **stopServer** command, see the stopServer command topic on the WebSphere Application Server, Version 8.0 information center.

7. Navigate to the *install_root*/BusinessSpace/config.bspace/MetadataFiles directory and depending on the database type that you will be using for Business Space, copy the relevant file to a working directory. Do not change the extension of this file: it must be .properties.
   a. Edit the copy of this file and modify the values to correspond to your database. Pay special attention to property **wasHome** and make sure that it is correct.
   b. When you have completed editing this file with your database information, save it.

After you have created the profiles and configured the database information for your profiles, you can configure Business Space in your environment by completing the following steps.

1. For each cluster or managed server run the **installBusinessSpace** command to install the Business Space enterprise archive (EAR) files in your runtime environment. Provide either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. See "Configuring Business Space using the command line" on page 191.
2. For each cluster or managed server, run the **configureBusinessSpace** command providing either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. Also specify the **bspacedbDesign** parameter. The value for this parameter should be the path to the database properties file that you previously edited. Optionally, if you want to create database tables and configure the Business Space database, specify the **createTables** parameter as true. See "Configuring Business Space using the command line" on page 191.
3. Save the wsadmin configuration.
4. If the **createTables** parameter was not specified in step 2, create and configure the Business Space database. See "Configuring the Business Space database" on page 193.
5. Start the deployment manager.
6. Start the clusters or managed servers.

If you augment to a profile that already has security set up with a user repository that is not the default federated repositories option, you must check the ConfigServices.properties file to adjust the MashupAdminForOOBSpace parameter. See "Selecting the user repository for Business Space" on page 216.

*Augmenting Business Space profiles for a network deployment configuration using the manageprofiles command-line utility:*

You can augment Business Space profiles for a network deployment configuration from the command line using the manageprofiles command-line utility.

Before you run the **manageprofiles** command-line utility to augment a profile, make sure that you have completed the following tasks:

- Review the full list of prerequisites for creating or augmenting a profile at Profile concepts in the WebSphere Application Server information center.
- Review example profile creation commands.

- Verify that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.
- Shut down any servers associated with the profile that you plan to augment.
- Determine if the profile you plan to augment has already been federated to a deployment manager. If the profile you want to augment has already been federated to a deployment manager, you cannot augment it using the manageprofiles command-line utility.
- Determine the template that the existing profile was created with (deployment manager, stand-alone, or managed). You can determine the template that was used for creating the profile by viewing the profile registry in *install_root*/properties/profileRegistry.xml. Do not modify this file, use it only to view the templates. For this procedure it is assumed that you are augmenting a Business Space powered by WebSphere deployment manager profile.

To use the **manageprofiles** command-line utility to augment a Business Space profile for a network deployment configuration, perform the following steps. This procedure assumes that you have an existing deployment manager profile and custom profiles (managed nodes) that you want to augment to Business Space.

If Business Space is augmented as part of your product profile, this task is optional.

1. Augment the deployment manager profile.
   a. Locate the dmgr.bspace template for Business Space deployment manager profiles, which define deployment managers. A deployment manager provides one administrative interface to a logical group of servers on one or more workstations.

      Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.

   b. Determine which parameters are required for augmenting the profile by reviewing the "manageprofiles command-line utility (for Business Space profiles)" on page 169 topic. Determine the values that you want to supply for the profile by reviewing the default values to see if they are what you need for your profile.

      You use the **augment** parameter to make changes to an existing profile with an augmentation template. The **augment** parameter causes the **manageprofiles** command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment. Make sure that you specify the fully qualified file path for **-templatePath**, because a relative file path results in the specified profile not being fully augmented.

   c. Run the file from the command line. Here is a simple example:

      ```
      manageProfiles -augment -profileName profile_name
       -templatePath install_root/profileTemplates/BusinessSpace/dmgr.bspace
       -serverType DEPLOYMENT_MANAGER -cellName management_cell_name
       -nodeName management_node_name -enableAdminSecurity true
       -adminUserName admin_user_name -adminPassword admin_password
      ```

      The command displays status as it runs. Wait for it to finish.
2. Start the deployment manager profile.

   Start the profile using the **startServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **startServer.sh** *server_name*
   - Windows **startServer.bat** *server_name*

   For more information about the **startServer** command, see the startServer command topic on the WebSphere Application Server, Version 8.0 information center.
3. Augment the custom profiles (managed nodes).

a. Locate the managed.bspace template for Business Space custom profiles, which, when federated to a deployment manager, define managed nodes. If you have decided that your solution requires a deployment environment, your runtime environment requires one or more managed nodes. A custom profile contains an empty node that you must federate into a deployment manager cell to make operational. Federating the custom profile changes it into a managed node. Do not federate a node unless the deployment manager you are federating to is at a release level the same or higher than that of the custom profile you are creating.

   Templates for each profile are located in the *install_root*/profileTemplates/BusinessSpace directory.

b. Determine which parameters are required for augmenting the profile by reviewing the "manageprofiles command-line utility (for Business Space profiles)" on page 169 topic. Determine the values that you want to supply for the profile by reviewing the default values to see if they are what you need for your profile.

   You use the **augment** parameter to make changes to an existing profile with an augmentation template. The **augment** parameter causes the **manageprofiles** command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment. Make sure that you specify the fully qualified file path for **-templatePath**, because a relative file path results in the specified profile not being fully augmented.

c. Run the file from the command line. Here is a simple example:

```
manageProfiles -augment -profileName profile_name
 -templatePath install_root/profileTemplates/BusinessSpace/managed.bspace
 -dmgrAdminUserName admin_user_name -dmgrAdminPassword admin_password
 -dmgrPort deployment_manager_port -dmgrHost deployment_manager_host_name -cellName
 management_cell_name -nodeName node_name
```

   The command displays status as it runs. Wait for it to finish.

4. Log on to the deployment manager administrative console.
5. Optional: If you don't already have a cluster or managed servers, do one of the following for your environment:
   - For a cluster:
     a. Create an application server cluster.
     b. Add one or more cluster members to the cluster (these are the Business Space custom profiles that were previously created).
   - For each managed server:
     a. Create an application server.
     b. Select the managed server's node to be the Business Space custom profile that was previously created.
6. Stop the deployment manager profile.

   Stop the deployment manager using the **stopServer** command from the *profile_root*/bin directory.

   Use the following syntax:

   - Linux UNIX **stopServer.sh** *server_name* **-username** *user_name* **-password** *password*
   - Windows **stopServer.bat** *server_name* **-username** *user_name* **-password** *password*

   If the profile does not have security enabled the **-username** and **-password** parameters are not necessary.

   For more information about the **stopServer** command, see the stopServer command topic on the WebSphere Application Server, Version 8.0 information center.
7. Navigate to the *install_root*/BusinessSpace/config.bspace/MetadataFiles directory and depending on the database type that you will be using for Business Space, copy the relevant file to a working directory. Do not change the extension of this file: it must be .properties.

a. Edit the copy of this file and modify the values to correspond to your database. Pay special attention to property **wasHome** and make sure that it is correct.
b. When you have completed editing this file with your database information, save it.

After you have created the profiles and configured the database information for your profiles, you can configure Business Space in your environment by completing the following steps.

1. For each cluster or managed server run the **installBusinessSpace** command to install the Business Space enterprise archive (EAR) files in your runtime environment. Provide either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. See "Configuring Business Space using the command line" on page 191.
2. For each cluster or managed server, run the **configureBusinessSpace** command providing either a **clusterName** parameter or **nodeName** and **serverName** parameters, depending on how you set up your network deployment topology. Also specify the **bspacedbDesign** parameter. The value for this parameter should be the path to the database properties file that you previously edited. Optionally, if you want to create database tables and configure the Business Space database, specify the **createTables** parameter as true. See "Configuring Business Space using the command line" on page 191.
3. Save the wsadmin configuration.
4. If the **createTables** parameter was not specified in step 2, create and configure the Business Space database. See "Configuring the Business Space database" on page 193.
5. Start the deployment manager.
6. Start the clusters or managed servers.

If you augment to a profile that already has security set up with a user repository that is not the default federated repositories option, you must check the `ConfigServices.properties` file to adjust the MashupAdminForOOBSpace parameter. See "Selecting the user repository for Business Space" on page 216.

*manageprofiles command-line utility (for Business Space profiles):*

The **manageprofiles** command-line utility creates a profile, which is the set of files that define the runtime environment for a deployment manager, a managed node, or a stand-alone server. You can use it to create a Business Space powered by WebSphere profile. If Business Space is configured as part of your product profile, this information is optional.

The profile defines the runtime environment and includes all of the files that the server processes can change during run time.

The **manageprofiles** command-line utility and its graphical user interface, the Profile Management Tool, are the only ways to create profiles, or the only ways to create runtime environments. You can also augment profiles and delete profiles with the **manageprofiles** command-line utility.

The command file is located in the *install_root*`/bin` directory. The command file is a script named `manageprofiles.sh` for Linux and UNIX operating systems or `manageprofiles.bat` for Windows operating systems.

The **manageprofiles** command-line utility creates a log for every profile that it creates, deletes, or augments. The logs are in the following directory, depending on the operating system:

- Linux UNIX *install_root*`/logs/manageprofiles`
- Windows *install_root*`\logs\manageprofiles`

The following file names are used:

- *profile_name*`_create.log`

- *profile_name*_augment.log
- *profile_name*_delete.log

Templates for each profile are located in the install_root/profileTemplates/BusinessSpace directory. Within this directory are various directories that correspond to different profile types. The directories are the paths that you indicate while using the **manageprofiles** command-line utility with the -templatePath option. You can also specify profile templates that lie outside the installation root if they exist. Use the following templates with BusinessSpace:

- default.bspace: for a BusinessSpace stand-alone server profile, which defines a stand-alone server.
- dmgr.bspace: for a BusinessSpace deployment manager profile, which defines a deployment manager.
- managed.bspace: for a BusinessSpace custom profile, which, when federated to a deployment manager, defines a managed node.

**Syntax**

Use the **manageprofiles** command-line utility to complete the following tasks:

- Creating a profile (**-create** parameter).
- Augmenting a profile (**-augment** parameter).

  **Restriction:** Using profiles that have been unaugmented (**-unaugment** parameter) is not supported.
- Deleting a profile (**-delete** parameter).
- Deleting all profiles (**-deleteAll** parameter)
- Listing all profiles (**-listProfiles** parameter)
- Getting the name of an existing profile from its name (**-getName** parameter)
- Getting the name of an existing profile from its path (**-getPath** parameter)
- Validating a profile registry (**-validateRegistry** parameter)
- Validating and updating a profile registry (**-validateAndUpdateRegistry** parameter)
- Getting the default profile name (**-getDefaultName** parameter)
- Setting the default profile name (**-setDefaultName** parameter)
- Backing up a profile (**-backupProfile** parameter)
- Restoring a profile (**-restoreProfile** parameter)
- Using a response file containing the information required to run a **manageprofiles** command-line utility (**-response** parameter)

For detailed help including the required parameters for each of the tasks accomplished with the **manageprofiles** command-line utility, use the **-help** parameter. The following example uses the **-help** parameter with the **manageprofiles** command-line utility **-augment** parameter on Windows operating systems: **manageprofiles.bat -augment -help**. The output specifies which parameters are required and which are optional.

**Command output**

On completion, the command displays a statement similar to one of the following messages. (Exact wording varies depending on whether you created, deleted or augmented a profile.)

- **INSTCONFSUCCESS**: Profile creation succeeded.
- **INSTCONFFAILED**: Profile creation failed.
- **INSTCONFPARTIALSUCCESS**: Some noncritical post installation configuration actions did not succeed.

In some cases, the statement is displayed more than once. For example, the **INSTCONFSUCCESS** line is displayed three times at the command line. For more information, see "Installation and profile creation log files."

**Parameters**

When creating a BusinessSpace profile, use only the parameters that are documented in the information center for BusinessSpace. All parameters are case-sensitive.

**-adminUserName** *adminUser_ID*
Specifies the user ID that is used for administrative security. For augmenting an existing profile that has administrative security enabled, this parameter is required.

**-adminPassword** *adminPassword*
Specifies the password for the administrative security user ID specified with the **-adminUserName** parameter. For augmenting an existing profile that has administrative security enabled, this parameter is required.

**-augment**
Use the **-augment** parameter to make changes to an existing profile with an augmentation template. The **-augment** parameter causes the **manageprofiles** command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment.

**Important:** Do not manually modify the files that are located in the *install_dir*/profileTemplates directory. For example, if you are changing the ports during profile creation, use the Profile Management Tool or the **-startingPort** or **-portsFile** arguments on the **manageprofiles** command-line utility instead of modifying the file in the profile template directory.
Specify the fully qualified file path for **-templatePath**. For example: **manageprofiles(.bat)(.sh) -augment -profileName profile_name -templatePath fully_qualified_template_path**

**-backupProfile**
Performs a file system back up of a profile folder and the profile metadata from the profile registry file.

**-backupFile** *backupFile_name*
Backs up the profile registry file to the specified file. You must provide a fully qualified file path for the *backupFile_name*.

**-bspacedbDesign** *db_design_file*
Specifies the path to the Business Space database design file. Sample design files are found in *install_root*/BusinessSpace/config.bspace/MetadataFiles.

**-bspaceSchemaName** *db_schema_name*
The schema name for the database. If no value is specified, for most database types, **IBMBUSSP** is used.

**-cellName** *cell_name*
Specifies the cell name of the profile. Use a unique cell name for each profile. When augmenting a profile, specify the cell of the original profile.The default value for this parameter is based on a combination of the short host name, the constant **Cell**, and a trailing number, for example:

```
if (DMgr)
    shortHostNameCellCellNumber
else
    shortHostNameNodeNodeNumberCell
```

where *CellNumber* is a sequential number starting at 01 and *NodeNumber* is the node number that you used to define the node name. The value for this parameter must not contain spaces or any characters that are not valid such as the following: *, ?, ", <, >, ,, /, \, and |.

**-create**
Creates the profile. Specify **manageprofiles -create -templatePath fully_qualified_file_path_to_template -help** for specific information about creating a profile. Available templates include:

- default.bspace: for a BusinessSpace stand-alone server profile, which defines a stand-alone server.
- dmgr.bspace: for a BusinessSpace deployment manager profile, which defines a deployment manager.
- managed.bspace: for a BusinessSpace custom profile, which, when federated to a deployment manager, defines a managed node.
-

**-dbBSpacePassword** *bspace_db_pswd*
This parameter is required if you enter a user-specified user name and password during profile creation and if you specify**ORACLE** for **dbType**. The default is **dbPassword**.

**-dbBSpaceUserId** *bspace_db_userid*
This parameter is required if you enter a user-specified user name and password during profile creation. The default is **IBMBUSSP**.

**-dbConnectionLocation** *db2_location*
The location of DB2 for z/OS database.

**-dbCreateNew**
Indicates if you will create or reuse a database. Valid values are **true** or **false**. The default value is **true**.

**-dbDelayConfig**
Indicates if you will postpone table creation until after the profile is created. Valid values are **true** or **false**. The default value is **false**. Set this parameter to **true** to delay execution of database scripts if using a remote database.

**-dbDriverType** *db_driver_type*
The database driver type that is valid only for Oracle. For an Oracle database, specify `ORACLE`. For databases other than Oracle, the value is automatically set based on the server operating system. Server installations on z/OS use type 2. Server installations on all other operating systems use type 4.

**-dbDriverVersion** *db_driver_version*
The database driver version that is valid only for Microsoft SQL Server. For a SQL Server database, specify either 1.2 for Microsoft SQL JDBC driver 1.2 or 2.0 for Microsoft SQL JDBC driver 2.0. This value is automatically defaulted to 2.0 if not specified.

**-dbHostName** *db_host_name*
The database server host name or IP address. The default value is **localhost**.

**-dbJDBCClasspath** *jdbc_driver_location*
The location of JDBC driver files. You must install the `ojdbc6.jar` driver to access the Oracle database. Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.

**-dbName** *db_name*
The name of the database. By default, the value is set to **orcl** for Oracle databases and to **BSPACE** for all other supported databases.

**-dbPassword** *db_pswd*
The password required for all database authentication.

**-dbServerPort** *db_port_number*
The database server port number. Depending on the database you are using, you can specify a different port number instead of the default port number.

**-dbStorageGroup** *db_stg_group*
The storage group name for DB2 z/OS databases.

**-dbSysPassword** *sys_pwd*
Use this parameter when **dbDelayConfig** is set to false and if you specified `ORACLE` for **dbType**. The parameter is optional. If not specified, the Oracle schema will not be created.

**-dbSysUserId** *sys_user_id*
This ID must have SYSDBA privileges. Do not use the Oracle internal user **sys**. Use this parameter when **dbDelayConfig** is set to false and if you specified `ORACLE` for **dbType**. The parameter is optional. If not specified, the Oracle schema will not be created.

**-dbType** *db_type*
The database type. Set one of the following values for the type of database product you are using with Business Space.

- DB2 DataServer = DB2_DataServer
- DB2 Universal for z/OS = DB2UDBOS390
- Oracle = Oracle
- Microsoft SQL Server = MSSQLSERVER_MICROSOFT

**-dbUserId** *db_userid*
User ID for all database types. Specifies the user ID that has privileges to create and drop the databases. The WebSphere data source uses this ID to authenticate the database connection. For DB2 databases, it specifies the database user ID that will own the database tables. For DB2 for z/OS databases, it specifies the user ID that has privileges to create and drop the databases. This parameter is required. Important: The **-dbUserId** parameter value must be a valid database authorization ID. For more information on authorization IDs, refer to the Authorization IDs and authorization names section of the DB2 property restriction page.

**-dbWinAuth true|false**
Specifies if you are using Windows Authentication with Microsoft SQL Server. If you want to use Windows Authentication in your SQL Server environment, you must specify this parameter as**true**. The default is **false**.

**-debug**
Turns on the debug function of the Apache Ant utility, which the **manageprofiles** command-line utility uses.

**-defaultPorts**
Assigns the default or base port values to the profile.

Do not use this parameter when using the **-startingPort** or **-portsFile** parameter.

During profile creation, the **manageprofiles** command-line utility uses an automatically generated set of recommended ports if you do not specify the **-startingPort** parameter, the **-defaultPorts** parameter or the **-portsFile** parameter. The recommended port values can be different than the default port values based on the availability of the default ports.

**Note:** Do not use this parameter if you are using the managed profile template.

**-delete**
Deletes the profile.

Deleting a profile does not delete the profile directory. For example, if you create a profile in the `/usr/WebSphere/AppServer/profiles/AppSrvr01` directory, the directory remains after you delete the profile.

You can delete or leave the directory. However, the *profile_root*`/logs` directory contains information about uninstalling the profile. For example, you might retain the `_nodeuninst.log` file to determine the cause of any problem during the uninstallation procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

**-deleteAll**
Deletes all registered profiles.

Deleting a profile does not delete the profile directory. For example, suppose that you create a profile in the /usr/WebSphere/AppServer/profiles/AppSrvr01 directory, the directory remains after you delete the profile.

You can delete or leave the directory. However, the *profile_root*/logs directory contains information about uninstalling the profile. For example, you might retain the _nodeuninst.log file to determine the cause of any problem during the uninstallation procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

**-dmgrAdminUserName** *user_name*
If administrative security is enabled on the deployment manager, specify a valid user name.

**-dmgrAdminPassword** *password*
If administrative security is enabled on the deployment manager, specify a password for the user name.

**-dmgrHost** *deployment_manager_host_name*
Identifies the workstation where the deployment manager is running. Specify this parameter and the **dmgrPort** parameter to federate a custom profile as it is created or augmented. This parameter is available with the managed.bspace profile template.

The host name can be the long or short DNS name or the IP address of the deployment manager workstation.

Specifying this optional parameter directs the **manageprofiles** command-line utility to attempt to federate the custom node into the deployment manager cell as it creates the custom profile. This parameter is ignored when creating a deployment manager profile or stand-alone server profile.

If you federate a custom node when the deployment manager is not running, the installation indicator in the logs is **INSTCONFFAILED** to indicate a complete failure. The resulting custom profile is unusable. You must move the custom profile directory out of the profile repository (the profile's installation root directory) before creating another custom profile with the same profile name.

If you have changed the default JMX connector type, you cannot federate with the **manageprofiles** command-line utility. Use the **addNode** command instead.

The default value for this parameter is **localhost**. The value for this parameter must be a properly formed host name and must not contain spaces or characters that are not valid such as the following characters: *, **?**, ", <, >, , , /, \, and |. A connection to the deployment manager must also be available in conjunction with the **dmgrPort** parameter.

**-dmgrPort** *deployment_manager_port_number*
Identifies the SOAP port of the deployment manager. Specify this parameter and the **dmgrHost** parameter to federate a custom profile as it is created or augmented. The deployment manager must be running and accessible.

If you have changed the default JMX connector type, you cannot federate with the **manageprofiles** command-line utility. Use the **addNode** command instead.

The default value for this parameter is **8879**. The port that you indicate must be a positive integer and a connection to the deployment manager must be available in conjunction with the **dmgrHost** parameter.

**-enableAdminSecurity true | false**
Enables administrative security. Valid values include **true** or **false**. The default value is **false**. If you

are creating profiles for a deployment environment, you must set this parameter to **true**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

When **enableAdminSecurity** is set to **true**, you must also specify the parameters **-adminUserName** and **-adminPassword** along with the values for these parameters. If samples were installed during the application server installation, you must also specify the **-samplesPassword** parameter when creating a profile for which administrative security is enabled. If the **-samplesPassword** parameter is not specified when administrative security is enabled, the profile is created successfully, but when you attempt to run the samples, exceptions and failures will be put in the server system out log.

Linux

**-enableService true | false**
Enables the creation of a Linux service. Valid values include **true** or **false**. The default value for this parameter is **false**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

When the **manageprofiles** command-line utility is run with the `-enableService` option set to **true** , the Linux service is created with the profile when the command is run by the root user. When a nonroot user runs the **manageprofiles** command-line utility, the profile is created, but the Linux service is not. The Linux service is not created because the nonroot user does not have sufficient permission to set up the service. An **INSTCONPARTIALSUCCESS** result is displayed at the end of the profile creation and the profile creation log *install_root*`/logs/manageprofiles/`*profile_name*`_create.log` contains a message indicating the current user does not have sufficient permission to set up the Linux service.

**-federateLater true | false**
Indicates if the managed profile will be federated during profile creation or if you will federate it later using the **addNode** command. If you are creating a Business Space profile, do not supply a value; use the default of **true**.

**-getDefaultName**
Returns the name of the default profile.

**-getName**
Gets the name for a profile registered at a given **-profilePath** parameter.

**-getPath**
Gets the file system location for a profile of a given name. Requires the **profileName** parameter.

**-help**
Displays command syntax.

**-hostName** *host_name*
Specifies the host name where you are creating the profile. Do not supply this parameter when augmenting an existing profile. This should match the host name that you specified during installation of the initial product. The default value for this parameter is the long form of the domain name system. This parameter is required for profile creation only. The value for this parameter must be a valid IPv6 host name and must not contain spaces or any characters that are not valid such as the following characters: *, ?, ", <, >, ,, /, \, and |.

**-importPersonalCertKS** *keystore_path*
Specifies the path to the keystore file that you use to import a personal certificate when you create the profile. The personal certificate is the default personal certificate of the server.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the **manageprofiles** utility adds the public key of the personal certificate to the `trust.p12` file and creates a root signing certificate.

The **-importPersonalCertKS** parameter is mutually exclusive with the **-personalCertDN** parameter. If you do not specifically create or import a personal certificate, one is created by default.

When you specify any of the parameters that begin with **-importPersonal**, you must specify them all.

**-importPersonalCertKSType** *keystore_type*
Specifies the type of the keystore file that you specify on the **-importPersonalCertKS** parameter. Values might be **JCEKS**, **CMSKS**, **PKCS12**, **PKCS11**, and **JKS**. However, this list can change based on the provider in the `java.security` file.

When you specify any of the parameters that begin with **-importPersonal**, you must specify them all.

**-importPersonalCertKSPassword** *keystore_password*
Specifies the password of the keystore file that you specify on the **-importPersonalCertKS** parameter.

When you specify any of the parameters that begin with **-importPersonal**, you must specify them all.

**-importPersonalCertKSAlias** *keystore_alias*
Specifies the alias of the certificate that is in the keystore file that you specify on the **-importPersonalCertKS** parameter. The certificate is added to the server default keystore file and is used as the server default personal certificate.

When you specify any of the parameters that begin with **-importPersonal**, you must specify them all.

**-importSigningCertKS** *keystore_path*
Specifies the path to the keystore file that you use to import a root certificate when you create the profile. The root certificate is the certificate that you use as the server default root certificate. The **-importSigningCertKS** parameter is mutually exclusive with the **-signingCertDN** parameter. If you do not specifically create or import a root signing certificate, one is created by default.

When you specify any of the parameters that begin with **-importSignin**g, you must specify them all.

**-importSigningCertKSType** *keystore_path*
Specifies the type of the keystore file that you specify on the **-importSigningCertKS** parameter. Valid values might be **JCEKS**, **CMSKS**, **PKCS12**, **PKCS11**, and **JKS**. However, this list can change based on the provider in the `java.security` file.

When you specify any of the parameters that begin with **-importSigning**, you must specify them all.

**-importSigningCertKSPassword** *keystore_password*
Specifies the password of the keystore file that you specify on the **-importSigningCertKS** parameter.

When you specify any of the parameters that begin with **-importSigning**, you must specify them all.

**-importSigningCertKSAlias** *keystore_alias*
Specifies the alias of the certificate that is in the keystore file that you specify on the **-importSigningCertKS** parameter. The certificate is added to the server default root keystore and is used as the server default root certificate.

When you specify any of the parameters that begin with **-importSigning**, you must specify them all.

**-isDefault**
Specifies that the profile identified by the accompanying **-profileName** parameter is to be the default profile once it is registered. When issuing commands that address the default profile, it is not necessary to use the **-profileName** attribute of the command.

**-keyStorePassword** *keyStore_password*
Specifies the password to use on all keystore files created during profile creation. Keystore files are created for the default personal certificate and the root signing certificate.

**-listAugments**
Lists the registered augments on a profile that is in the profile registry. You must specify the **-profileName** parameter with the **-listAugments** parameter.

**-listProfiles**
Lists all defined profiles.

**-nodeName** *node_name*
Specifies the node name for the node that is created with the new profile. Use a unique value within the cell or on the workstation. Each profile that shares the same set of product binaries must have a unique node name. When augmenting a profile, specify the node of the original profile.

Linux UNIX Windows The default value for this parameter is based on the short host name, profile type, and a trailing number, for example:

```
if (DMgr)
 shortHostNameCellManagerNodeNumber
else
 shortHostNameNodeNodeNumber
```

where *NodeNumber* is a sequential number starting at **01**.

The value for this parameter must not contain spaces or any characters that are not valid such as the following characters: *, ?, ", <, >, ,, /, \, and |, .

**-omitAction** *feature1 feature2... featureN*
An optional parameter that excludes profile features.

Each profile template comes predefined with certain optional features. The **samplesInstallAndConfig** option is only available when the product is installed with samples applications selected. The following optional features can be used with the **-omitAction** parameter for the following profile templates:

- **default** - Application server
  - deployAdminConsole
  - samplesInstallAndConfig
  - defaultAppDeployAndConfig
- **dmgr** - Deployment manager
  - deployAdminConsole

**-personalCertDN** *distinguished_name*
Specifies the distinguished name of the personal certificate that you are creating when you create the profile. Specify the distinguished name in quotation marks. This default personal certificate is located in the server keystore file. The **-importPersonalCertKSType** parameter is mutually exclusive with the **-personalCertDN** parameter. See the **-personalCertValidityPeriod** parameter and the **-keyStorePassword** parameter.

**-personalCertValidityPeriod** *validity_period*
An optional parameter that specifies the amount of time in years that the default personal certificate is valid. If you do not specify this parameter with the **-personalCertDN** parameter, the default personal certificate is valid for one year.

**-portsFile** *file_path*
An optional parameter that specifies the path to a file that defines port settings for the new profile. Do not supply this parameter when augmenting an existing profile.

Do not use this parameter when using the **-startingPort** or **-defaultPorts** parameter.

During profile creation, the **manageprofiles** command-line utility uses an automatically generated set of recommended ports if you do not specify the **-startingPort** parameter, the **-defaultPorts** parameter or the **-portsFile** parameter. The recommended port values can be different than the default port values based on the availability of the default ports.

**-profileName** *profile_name*
Specifies the name of the profile. Use a unique value when creating a profile.

Each profile that shares the same set of product binaries must have a unique name. The default profile name is based on the profile type and a trailing number, for example:

```
profileType ProfileNumber
```

where *profileType* is a value such as **AppSrv**, **Dmgr**, or **Custom** and *ProfileNumber* is a sequential number that creates a unique profile name.
The value for this parameter must not contain spaces or characters that are not valid such as the following characters: *, ?, ", <, >, ,, /, \, and |. The profile name that you choose must not be in use.

**-profilePath** *profile_root*
Specifies the fully qualified path to the profile, which is referred to throughout the information center as the *profile_root*.

For example:

```
-profilePath profile_root
```

Use this parameter when creating profiles only. Do not set this parameter for augmenting an existing profile.

Windows **On Windows operating systems:** If the fully qualified path contains spaces, enclose the value in quotation marks.

The default value is based on the *install_root* directory, the profiles subdirectory, and the name of the file.

For example, the default for profile creation is:

```
WS_WSPROFILE_DEFAULT_PROFILE_HOME/profileName
```

where *WS_WSPROFILE_DEFAULT_PROFILE_HOME* is defined in the `wasprofile.properties` file in the *install_root*`/properties` directory.

The value for this parameter must be a valid path for the target system and must not be currently in use.

You must have permissions to write to the directory.

**-response** *response_file*
Accesses all API functions from the command line using the **manageprofiles** command-line utility.

The command line interface can be driven by a response file that contains the input arguments for a given command in the properties file in key and value format. The following is an example response file for a create operation:

```
create
profileName=testResponseFileCreate
profilePath=profile_root
templatePath=install_root/profileTemplates/default
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

Windows **On Windows operating systems:** The path statement in the Windows operating system can use either forward slashes (/) or back slashes (\). If the path statement uses back slashes, then the response file requires double back slashes for the response file to correctly understand the path. Here is an example of a response file for a create operation that uses the double back slashes:

```
create
templatePath=C:\\WebSphere\\AppServer\\profileTemplates\\BusinessSpace\\default.bspace
```

When adding properties that denote distinguished names for certificates, commas must be preceded by double back slashes (\\). Note that the separator between the key (**personalCertDN**) and the value is not an equals sign, it is a blank space. This is because the equals sign occurs within the property value. Here is an example of a response file cert entry statement using double back slashes:

```
personalCertDN cn=machine_name.dnx_suffix.com\\,ou=machine_name
Node04Cell\\,ou=machine_nameNode04\\,o=IBM\\,c=US
```

To determine which input arguments are required for the various types of profile templates and action, use the **manageprofiles** command-line utility with the **-help** parameter.

**-restoreProfile**
Restores a profile backup. Must be used with the **-backupFile** parameter.

**-samplesPassword** *samplesPassword*
Creates a password to be used for samples. The password is used to restrict access to web application samples installed during the installation of the application server.

**-serverType DEPLOYMENT_MANAGER**
Specifies the type of management profile. Specify `DEPLOYMENT_MANAGER` for a management profile. This parameter is required when you create a management profile.

Linux

**-serviceUserName** *service_user_ID*
Specifies the user ID that is used during the creation of the Linux service so that the Linux service will run under this user ID. The Linux service runs whenever the user ID is logged on.

**-setDefaultName**
Sets the default profile to one of the existing profiles. Must be used with the **-profileName** parameter, for example:

```
manageprofiles(.bat)(.sh) -setDefaultName -profileName profile_name
```

**-signingCertDN** *distinguished_name*
Specifies the distinguished name of the root signing certificate that you create when you create the profile. Specify the distinguished name in quotation marks. This default personal certificate is located in the server keystore file. The *-importSigningCertKS* parameter is mutually exclusive with the *-signingCertDN* parameter. If you do not specifically create or import a root signing certificate, one is created by default. See the *-signingCertValidityPeriod* parameter and the *-keyStorePassword*.

**-signingCertValidityPeriod** *validity_period*
An optional parameter that specifies the amount of time in years that the root signing certificate is valid. If you do not specify this parameter with the *-signingCertDN* parameter, the root signing certificate is valid for 20 years.

**-startingPort** *startingPort*
Specifies the starting port number for generating and assigning all ports for the profile.

Do not set this parameter if you are augmenting an existing profile. Port values are assigned sequentially from the **-startingPort** value, omitting those ports that are already in use. The system recognizes and resolves ports that are currently in use and determines the port assignments to avoid port conflicts.

Do not use this parameter with the **-defaultPorts** or **-portsFile** parameters.

During profile creation, the **manageprofiles** command-line utility uses an automatically generated set of recommended ports if you do not specify the **-startingPort** parameter, the **-defaultPorts** parameter or the **-portsFile** parameter. The recommended port values can be different than the default port values based on the availability of the default ports.

**Note:** Do not use this parameter if you are using the managed profile template.

**-templatePath** *template_path*
Specifies the directory path to the template files in the installation root directory. Within the `profileTemplates` directory are various directories that correspond to different profile types and that vary with the type of product installed. The profile directories are the paths that you indicate while using the **-templatePath** option. You can specify profile templates that lie outside the installation root, if you have any.

Use absolute paths. This parameter must exist as a directory and point to a valid template directory. Use the following templates with Business Space:
- `default.bspace`: for a Business Space stand-alone server profile, which defines a stand-alone server.
- `dmgr.bspace`: for a Business Space deployment manager profile, which defines a deployment manager.
- `managed.bspace`: for a Business Space custom profile, which, when federated to a deployment manager, defines a managed node.

**-validateAndUpdateRegistry**
Checks all of the profiles that are listed in the profile registry to see if the profiles are present on the file system. Removes any missing profiles from the registry. Returns a list of the missing profiles that were deleted from the registry.

**-validateRegistry**
Checks all of the profiles that are listed in the profile registry to see if the profiles are present on the file system. Returns a list of missing profiles.

**-validatePorts**
Specifies the ports should be validated to ensure they are not reserved or in use. Use this parameter to identify ports that are not being used. If a port is determined to be in use, the profile creation stops and an error message displays. You can use this parameter at any time on the create command line. It is recommended to use this parameter with the **portsFile** parameter.

**-webFormConfig true | false**
Indicates if Business Space is configured to use IBM Forms Server to work with Human Task Management widgets. The default value for this parameter is **false**. Indicate **true** to configure Business Space to use IBM Forms Server. Both the **webFormConfig** and **webFormInstallRoot** parameters are required to configure IBM Forms Server. This parameter is valid for stand-alone server profiles only.

**Note:** IBM Forms Server configuration using these parameters is only valid for local IBM Forms Server installations.

**-webServerCheck true | false**
Indicates if you want to set up web server definitions. Valid values include **true** or **false**. The default value for this parameter is **false**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerHostname** *webserver_host_name*
The host name of the server. The default value for this parameter is the long host name of the local workstation. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerInstallPath** *webserver_installpath_name*
The installation path of the web server, local or remote. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

The default value for this parameter is dependent on the operating system of the local workstation and the value of the **webServerType** parameter. For example: AIX

```
webServerType=IHS: webServerInstallPath defaulted to /usr/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to ?
webServerType=APACHE: webServerInstallPath defaulted to ?
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

HP-UX

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
```

```
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

Linux

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

Solaris

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

Windows

```
webServerType=IHS: webServerInstallPath defaulted to C:\Program Files\IBM\HTTPServer
webServerType=IIS: webServerInstallPath defaulted to C:\
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to C:\
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

**-webServerName** *webserver_name*
The name of the web server. The default value for this parameter is **webserver1**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerOS** *webserver_operating_system*
The operating system from where the web server resides. Valid values include: **windows**, **linux**, **solaris**, **aix, hpux**, **os390**, and **os400**. Use this parameter with the **webServerType** parameter.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerPluginPath** *webserver_pluginpath*
The path to the plug-ins that the web server uses. The default value for this parameter is ***install_root*/plugins**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerPort** *webserver_port*
Indicates the port from where the web server will be accessed. The default value for this parameter is **80**. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-webServerType** *webserver_type*
The type of the web server. Valid values include: **IHS**, **SUNJAVASYSTEM**, **IIS**, **DOMINO**, **APACHE**, and **HTTPSERVER_ZOS**. Use this parameter with the **webServerOS** parameter. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows

**-winserviceAccountType specifieduser | localsystem**
The type of the owner account of the Windows service created for the profile. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Valid values include **specifieduser** or **localsystem**. The **localsystem** value runs the Windows service under the local account of the user who creates the profile. The default value for this parameter is **system**.

Windows

**-winserviceCheck true | false**
The value can be either true or false. Specify **true** to create a Windows service for the server process that is created within the profile. Specify **false** to not create the Windows service. The default value for this parameter is **false**.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

**-winservicePassword** *winservice_password*
Specify the password for the specified user or the local account that is to own the Windows service. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows

**-winserviceStartupType manual | automatic | disabled**
Possible values for Windows service startup are:

- manual
- automatic
- disabled

The default value for this parameter is **manual**.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows

**-winserviceUserName** *winservice_user_ID*
Specify your user ID so that the Windows operating system can verify you as an ID that is authorized to create a Windows service. Your user ID must belong to the Administrator group and have the following advanced user rights:

- Act as part of the operating system
- Log on as a service

The default value for this parameter is the current user name. The value for this parameter must not contain spaces or characters that are not valid such as the following characters: *, **?**, ", <, >, ,, /, \, and |. The user that you specify must have the proper permissions to create a Windows service. You must specify the correct password for the user name that you choose.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

## Configuring Business Space as part of the Deployment Environment Configuration wizard

Business Space configuration and Representational State Transfer (REST) service configuration for widgets in Business Space are automatically included in the Deployment Environment Configuration wizard. You can decide which REST services to configure.

Before you begin this task, you must complete the following tasks:

- Install your product.
- Create a profile, making sure to designate a fully qualified host name for the profile.

- Enable security, if you want to set up a secured environment for Business Space.

If you are setting up deployment manager and custom profiles, this method is the simplest way to configure Business Space.

1. On the administrative console, click **Servers** > **Deployment Environments** > **New**. A series of pages in the wizard guides you through the process of creating your deployment environment.
2. Either define the new deployment environment or import a file that contains deployment environment definitions. You can create a deployment environment based on one of the IBM-supplied patterns or you can create a custom deployment environment.
3. On the Deployment Environment Patterns page, select one of the deployment environment patterns.
4. On the Select Nodes page, designate the nodes to participate in your deployment environment.
5. On the Clusters page, specify the number of cluster members from each node to assign to specific deployment environment functions.
6. On the Database page, configure the data source for Business Space, one of the components listed in the table. You can edit the description, test the connection, and set the database product you want to use for the Provider. If you want the Business Space tables to be automatically created and configured, select the **Create tables** check box. If you do not select the check box, you must manually configure the database for Business Space. The database product list contains all databases supported by each component.

   **Tip:** If you select the **Create tables** check box, make sure that the database has been created before creating the deployment environment.
7. On the Security page, configure the authentication aliases WebSphere uses when accessing secure components. The authentication alias user name and password can be changed on this page. These aliases are used to access secure components but do not provide access to data sources.
8. For IBM Business Process Manager configuration, supply information required to configure the application deployment target to support the deployment of the Business Process Choreographer components. Specify the context roots, security, and human task manager mail session values the wizard uses to configure Business Process Choreographer for this deployment environment.
9. For IBM Business Process Manager configuration, configure the business process rules manager to run on the cluster or server.
10. On the REST Services page, configure the services for the widgets you want available on Business Space for your runtime environment.
    - Type the port number and the host or virtual host that a client needs to communicate with the server or cluster. In a clustered environment, this is typically the load-balancing server host name and port.
    - If you leave the host and port fields empty, the values default to values of an individual cluster member host and its HTTP port. For a load-balanced environment, you must later change the default values to the virtual host name and port of the load-balancing server. Make sure to designate a fully qualified host name.
    - Set the description for the widgets if needed.

    .
11. On the next page, click **Finish** or **Finish and Generate Environment**.
12. Optional: If you did not select the **Create tables** check box on the Database page, run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. For more information, see Configuring the Business Space database.

**Tip:** Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. For more information, see Changing the timeout settings for the Business Space Ajax proxy.

## Configuring Business Space for network deployment environments

If you have a distributed or network deployment environment, configure Business Space using the administrative console or commands.

If you are using deployment manager and custom profiles, you must configure Representational State Transfer (REST) endpoints, configure Business Space, register the REST endpoints, and configure database tables.

**Configuring REST services:**

If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, Representational State Transfer (REST) services are configured and enabled automatically. For other environments, use the administrative console to configure the REST services.

If you want widgets to be available in Business Space, you must configure the REST services for those widgets. Later you must register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.

You can configure all REST services for a specific server or cluster. Or, you can select individual services to configure. You can manage individual service configuration by viewing all services for a service provider or by viewing all services for your environment.

REST services are typically exposed on the REST Gateway. Some REST services are implemented by their dedicated system application. The REST Services Gateway application enables common system REST services. The REST Services Gateway application is created when REST services are configured.

Make sure that the REST Services Gateway application is deployed for the particular scope that you are using. You configure REST services for the REST Services Gateway and other service providers by using the REST service providers configuration administrative console page. In order for some widgets to be enabled, you must do this on the scope where the widgets are running. The REST Services Gateway application is deployed to a specific scope when you add it on the REST service providers configuration administrative console page. To add a REST Services Gateway for a given scope, navigate to **Servers** > **Server types** > *my_server* > **Business Integration** > **REST services** or **Servers** > **Clusters** > *my_cluster* > **Business Integration** > **REST services**. Then configure the REST services gateway provider for the given server or cluster.

For clustered environments, all administration and configuration tasks for REST services are completed on the REST Services Gateway Dmgr application on the deployment manager. The REST Services Gateway Dmgr application is used with the following widgets:

- Module Browser
- Module Assembly
- Module Properties
- Proxy Gateway
- Module Health
- System Health

*Configuring all REST services on the administrative console:*

Configure all Representational State Transfer (REST) services for your environment by using the REST service administrative console page.

Before you complete this task, you must have installed your IBM business process management product.

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console page allows you to configure REST services for all of your product's widgets in Business Space. On the REST Services page, you can view all services for your environment and enable or disable each service individually.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use. To ensure that the REST endpoints are registered with Business Space, see Configuring Business Space and registering REST endpoints on the administrative console.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see Enabling Business Space widgets to work with multiple endpoints.

The REST Services Gateway application enables common system REST services. The REST Services Gateway application is created when REST services are configured.

1. Click **Services** > **REST services** > **REST services**.

   The REST Services page opens, displaying all REST services in your environment.
2. For the **Scope section**, designate all to view all REST services in your environment, or select a server or cluster where you have REST services enabled. If REST services that you expected to see for the selected scope are missing, enable the REST Services Gateway or the related REST service providers on the server or cluster. See Configuring REST services for a server, cluster or component.
3. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.
4. For each individual service that you want to enable, type a meaningful description in the **Description** column.
5. Click **OK** to commit the changes to the services.

- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

*Configuring REST services in a service provider:*

Configure Representational State Transfer (REST) services in a service provider by using the REST service providers configuration administrative console page.

Before you complete this task, you must have installed your IBM business process management product.

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console allows you to configure REST services for all of your product's widgets in Business Space. On the REST service providers configuration administrative console page, you can view all services for a selected service provider and enable or disable each service individually. This page allows you to manage individual service configuration by working with all services for a service provider.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use. To ensure that the REST endpoints are registered with Business Space, see Configuring Business Space and registering REST endpoints on the administrative console.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see Enabling Business Space widgets to work with multiple endpoints.

The REST Services Gateway application enables common system REST services. The REST Services Gateway application is created when REST services are configured.

The following REST service providers are available and are configured on the scope shown:

- **REST Services Gateway**: To add a REST Services Gateway for a given scope, navigate to **Servers** > **Server types** > *my_server* > **Business Integration** > **REST services** or **Servers** > **Clusters** > *my_cluster* > **Business Integration** > **REST services**. Configure the REST services gateway provider for the given server or cluster.
- **REST Services Gateway Dmgr**: The REST Services Gateway provider on the deployment manager is configured automatically when creating a deployment manager profile for IBM Business Process Manager or WebSphere Enterprise Service Bus. This provider hosts administrative REST services used by the Module Browser, Module Administration, Health Monitor and Proxy Gateway widgets.

1. Click **Services** > **REST services** > **REST service providers** .

   The REST service providers page opens, displaying all REST service providers.
2. Click a provider link to configure the services for the group of REST services managed by that provider.

   The REST service providers configuration page opens, displaying all REST services in the provider.
3. Select a **Protocol** from the list for all REST services that you want to configure so they are available in Business Space. Configure a full URL path by selecting either **https://** or **http://** and then completing the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port** fields. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space.
4. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.
5. For each individual service that you want to enable, type a meaningful description in the **Description** column.
6. Click **OK** to commit the changes to the services.

- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

*Configuring REST services for a server, cluster, or component:*

Configure Representational State Transfer (REST) services for a server, cluster or a component by using the REST Services administrative console page.

Before you complete this task, you must have installed your IBM business process management product.

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page allows you to configure services for a server, a cluster, or a component.

This task configures the REST service provider application for a particular server or cluster. You must configure the provider application before REST services are available on a server or cluster. For more on REST service providers, see Configuring REST services in a service provider.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use. To ensure that the REST endpoints are registered with Business Space, see Configuring Business Space and registering REST endpoints on the administrative console.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets to work with multiple endpoints."

The REST Services Gateway application enables common system REST services. The REST Services Gateway application is created when REST services are configured.

1. Click one of the following.
   - For REST services on a server, click: **Servers** > **Server Types** > **WebSphere application servers** > *name_of_server* > **Business Integration** > **REST Services**
   - For REST services on a cluster, click: **Servers** > **Clusters** > **WebSphere application server clusters** > *name_of_cluster* > **Business Integration** > **REST Services**

   The REST Services page appears, displaying all default REST services that you can configure for Business Space widgets for use with your product or component (Business Flow Manager or Human Task Manager). If a REST service has already been configured, you see a message displayed.
2. Select a **Protocol** from the list for all REST services that you want to configure so they are available in Business Space. Configure a full URL path by selecting either **https://** or **http://** and then completing the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port** fields. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space. This same restriction applies for all environments that use Flex-enabled Business Space widgets.
3. In the table of REST services, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.
4. In the table of REST services, type a meaningful description for each of the REST services in the **Description** field.
5. Click **OK** to commit the changes to the services.

   To modify the REST service configuration at a later time, you can come back to the REST Services page or you can use other administrative console pages to manage the configuration of REST service

endpoints. The REST service providers page allows you to select service provider that you want to configure. The REST services page accessed from **Services** > **REST services** allows you to configure all REST services in your environment.

- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

*Configuring REST services using the command line:*

All widgets required for your product are installed with Business Space powered by WebSphere. The Representational State Transfer (REST) services for widgets must be configured, enabled, and registered with Business Space before your team can use the widgets in Business Space. If you do not use the REST Services administrative console page, use the **updateRESTGatewayService** command.

Before you complete this task, you must have installed your IBM business process management product.

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page or the **updateRESTGatewayService** command allows you to configure services for REST application programming interfaces (APIs) for all of your product's widgets in Business Space.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets for multiple endpoints."

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.
2. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
3. Use the **updateRESTGatewayService** command to configure REST services specifying the cluster or the server and node. The **-enable** parameter is optional, and if not specified, defaults to true.
4. Run the save command.

The following example uses Jython to run the **updateRESTGatewayService** command and then save the changes. It configures the REST services on a cluster.

```
AdminTask.updateRESTGatewayService('[-clusterName
 cluster_name]')
AdminConfig.save()
```

The following example uses Jacl:

```
$AdminTask updateRESTGatewayService {-clusterName
 cluster_name}
$AdminConfig save
```

- Configure Business Space.

- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

**Configuring Business Space and registering REST endpoints on the administrative console:**

You can install and configure Business Space powered by WebSphere using the administrative console.

Before you begin this task, you must complete the following tasks:
- Install the product software and created a profile. When you install your product, Business Space files are included with the installation for the profiles that you set up. Your profile is not configured for Business Space until you explicitly configure Business Space on the profile.
- Enable security, if you want to set up a secured environment for Business Space.
- Configure Representational State Transfer (REST) services. If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, the REST service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST services. If you want widgets to be available in Business Space, you must configure the REST services for those widgets. On the Business Space Configuration administrative console page, you register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.
- If you want to configure Business Space on a server or cluster using a different data source than the product data source: Create the data source in the server or cluster scope with the correct JNDI name of jdbc/mashupDS before configuring Business Space using the administrative console.
- For Oracle, to use a different schema for the Business Space tables than the one used by the product database, complete the following steps to create a data source manually before you open the Business Space Configuration page:
  1. Create the schema using the database product software.
  2. Use the administrative console to configure the JDBC provider.
  3. Use the administrative console to create a data source with the JNDI name of jdbc/mashupDS at the server or cluster scope, depending on your environment.
  4. Use the administrative console to create an authentication alias. Set the user name to the schema you created and set the authentication according to your Oracle setup.
  5. Set the authentication alias on the data source.

If you are using deployment environments or other advanced profile configuration, you must use the administrative console to configure Business Space to work with your runtime environment. Business Space is a browser-based graphical user interface for the business users of the application that is running with the profile you set up. In Business Space, you can customize content from other IBM Business Process Manager products.

1. Ensure that the administrative console is running.
2. In the navigation pane click **Servers** > **Server Types** > **WebSphere application servers** or **Servers** > **Clusters** > **WebSphere application server clusters**.
3. Select the name of your server or cluster target.
4. On the Configuration page, under **Business Integration**, click **Business Space Configuration**. The Business Space Configuration page opens. If Business Space has already been configured, you can view this page, but you cannot edit the fields.
5. Select the **Install Business Space service** check box.

6. In the **Database schema name** box, type the name of the database schema that you want to use for the Business Space database.

   **Note:** In Oracle, the schema is the same as the user name set on the authentication alias on the data source.
7. If no data source is designated in the **Existing Business Space data source** field, go to **Create Business Space data source using** and select a data source that connects to the database you want to use with Business Space.

   Designating a data source under **Create Business Space data source using:** creates a data source for Business Space with a JNDI name of jdbc/mashupDS that is modeled on the data source you selected.

   The Business Space data source is created on the server or cluster on which you are configuring Business Space, even if the product data source is on a different server or cluster.

   **Tip:** If you do not see an existing data source that you want to use, you must cancel the Business Space Configuration page, set up the database and the data source that you want to use, and then restart the Business Space Configuration page to complete the configuration. For more information, see the Before you begin section.
8. Click **OK**.
9. To register the proper deployment target (cluster or server) for the system REST endpoints for each of the widgets you are using in Business Space, click **REST service endpoint registration**.

   The target that you select for a REST service endpoint type can set the scope of the data displayed in some widgets. Or, you might want to select a particular cluster or server for better performance or availability.

   If you are using Human Task Management widgets, you can select more than one REST service provider for a server or a cluster in the row for the Process Services and Task Services types. Select the provider with **Name=Federated REST Services**, the provider with **Name=Business Process Choreographer REST services**, or the provider with **Name=BPD engine REST services**. If you have tasks and processes running in both Business Process Choreographer and the business process definition (BPD) engine, select the federated REST services. If you are using only processes and tasks that are running in the Business Process Choreographer (modeled in Integration Designer), select the Business Process Choreographer REST services. If you are using only processes and tasks that are running in the BPD engine (modeled in Process Designer), select the BPD engine.

   If you do not specify the target, the REST endpoint of this type is not registered with Business Space, and any widgets that need the REST service endpoint of this type will not be visible in Business Space.
10. Save the configuration.
11. Run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. The scripts were generated when you completed the configuration. For more information, see Configuring the Business Space database.

**Note:** If you are using Oracle, the password of the authentication alias of the Business Space data source is set to same as the schema name of Business Space. The default value of the schema is IBMBUSSP. When you configure Business Space, you can specify a different schema on the administrative console or in the command line. In that case, the default password is the same as the schema you specify. If you want to use a different password for the Business Space user name, you must use the administrative console to updated JDBC Resources: Find the data source jdbc/mashupsDS. Modify the value of the authentication alias to make it match the password of the Business Space schema name. Save your changes and restart the server.

**Note:** Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your

REST services, depending on the performance of the REST service servers. For more information, see Changing the timeout settings for the Business Space Ajax proxy.

**Configuring Business Space using the command line:**

You can set up and configure Business Space powered by WebSphere using the **wsadmin** command. You can use the **wsadmin** command to perform the same configuration of Business Space that you can perform in the administrative console.

Before you begin this task, you must complete the following tasks:

- Install the product software and create a profile. When you install your product, Business Space files are included with the installation for the profiles that you set up. Your profile is not configured for Business Space until you explicitly configure Business Space on the profile.
- If you want to set up a secured environment for Business Space, enable security.
- If you plan to use a database design file for the Business Space database information, complete the steps in "Creating a Business Space database design properties file" on page 193.
- Configure Representational State Transfer (REST) services. If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, the REST service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST services. If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. You must register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.
- If you want to configure Business Space on a server or cluster using a different data source than the product data source, create the data source in the server or cluster scope with the correct JNDI name of jdbc/mashupDS before configuring Business Space (before running the **configureBusinessSpace** command).
- For Oracle, to use a different schema for the Business Space tables than the one used by the product database, complete the following steps to create a data source manually before you run the commands to install and configure Business Space in the procedure below:
  - Use the administrative console to configure the JDBC provider.
  - Use the administrative console to create a data source with the JNDI name of jdbc/mashupDS at the server or cluster scope, depending on your environment.

You can use the command line to configure Business Space if you want to write scripts instead of using the administrative console to configure Business Space.

If you are not sure whether Business Space is already configured, you can run the **getBusinessSpaceDeployStatus** command to check whether Business Space is configured on a server, cluster, or cell. For more information about that command, see "getBusinessSpaceDeployStatus command."

To configure Business Space, complete the following steps.

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.
2. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
3. Use the **installBusinessSpace** command to install the Business Space enterprise archive (EAR) files in your runtime environment.
4. Use the **configureBusinessSpace** command to configure the data source for Business Space and copy the scripts that configure the database tables to *profile_root*/dbscripts/BusinessSpace/

*node_name_server_name/database_type/database_name* for a stand-alone server or *profile_root*/dbscripts/BusinessSpace/*cluster_name/database_type/database_name* for a cluster.

If you did not specify the **createTables** parameter as true when running the **configureBusinessSpace** command, you must run the scripts that configure the database tables. For more information about the scripts, see "Configuring the Business Space database" on page 193.

If you are using a database design file for database configuration, you can use the **-bspacedbDesign** parameter to designate that file when you run the **configureBusinessSpace** command.

If you are using Windows Authentication with Microsoft SQL Server, make sure to specify the **-dbWinAuth** parameter as **true**.

5. After each command, run `AdminConfig.save(` (Jython) or `$AdminConfig save` (Jacl).
6. Run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. For more information, see Configuring Business Space database tables.

Configuring Business Space sets up a browser-based graphical user interface for the business users of your application that is running with the profile you set up. In Business Space, you and your application users can customize content from products in the WebSphere business process management portfolio.

The following example uses Jython to run the **installBusinessSpace** and **configureBusinessSpace** commands to install the EAR files and configure the data source for Business Space on a cluster. The example designates the schema and the product database to use with Business Space when multiple products are installed. In a situation where both IBM Business Process Manager and IBM Business Monitor are installed, this example creates a Business Space data source using the properties of the IBM Business Process Manager data source.

```
AdminTask.installBusinessSpace('[-clusterName myCluster -save
 true]')
AdminTask.configureBusinessSpace('[-clusterName
 myCluster -schemaName mySchema -productTypeForDatasource
 WPS -save true]')
```

The following example uses Jacl:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save
 true}
$AdminTask configureBusinessSpace {-clusterName
 myCluster -schemaName mySchema -productTypeForDatasource
 WPS -save true}
```

**Tip:** If you are using Oracle, the password of the authentication alias of the Business Space data source is set to the same name as the schema name of Business Space. The default value of the schema is IBMBUSSP. When you configure Business Space, you can specify a different schema on the administrative console or in the command line. In that case, the default password is the same as the schema you specify. If you want to use a different password for the Business Space user name, you must use the administrative console to updated JDBC Resources: Find the data source jdbc/mashupsDS. Modify the value of the authentication alias to make it match the password of the Business Space schema name. Save your changes and restart the server.

After configuring Business Space, you must complete the following steps to enable Business Space for your runtime environment.

- Register the endpoints with the **registerRESTserviceEndpoint** command.
- Set up security that you need to use with Business Space and the widgets your team is using. For more information, see "Setting up security for Business Space."

**Tip:** Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. For more information, see Changing the timeout settings for the Business Space Ajax proxy.

**Creating a Business Space database design properties file:**

If your Business Space database type is other than the default, create a database design properties file to simplify the database creation process.

Design file templates for each database type are provided in the *install_root*/BusinessSpace/config.bspace/MetadataFiles directory; for example, the design file template for DB2 is called BSpace_DB2-distributed.properties.

1. Create a new file by making a copy of the template file for your database type.
2. Change the values of the property settings in the database design properties file, according to your configuration. Comments are provided in the file to help you choose the correct property values.

Supply the full path of your database design properties file in one of the following locations, depending on your product environment and configuration preference:

- If you are using the profile management tool to configure Business Space with a profile, designate the database design file by selecting the **Use a database design file** option.
- If you are using the **manageprofiles** command-line utility to configure Business Space with a profile, designate the database design file with the **-bspacedbDesign** parameter.
- If you are using the **configureBusinessSpace** command to configure Business Space, designate the database design file with the **-bspacedbDesign** parameter.

**Configuring the Business Space database:**

You can manually install database tables for Business Space on a remote database server with scripts that are generated by the installation program. If you are using a deployment environment, or if your database is remote, you must install these tables after configuring Business Space.

Before you complete this task, you must complete the following tasks:

- Install the product.
- Create profiles and configure servers or clusters for Business Space.
- For Oracle: create the database.
- For Microsoft SQL Server: set SQL Server instance authentication. The SQL Server JDBC driver supports mixed authentication mode only. Therefore, when the SQL Server instance is created, the authentication must be set to **SQL Server and Windows**.
- For all databases, make sure that the database is installed using a UTF-8 Universal character set if you want to use Business Space in your environment.
- Make sure that your application server with Business Space is stopped.

If you are using DB2 for z/OS and the required resources have not already been set up as part of the core product installation, complete the following additional items before you begin this task:

- Create a TEMP database and a TEMP table space to contain the declared temporary tables for processing scrollable cursors.
- Create a dedicated STOGROUP to contain the Business Space data.

For DB2 for z/OS, if you want to use a different storage group (for example, if you do not want Business Space database tables to be added to the same database and storage group as the common database), you must edit and run the createTablespace_BusinessSpace.sql script after you configure Business Space and before you configure the Business Space database tables.

- Edit the createTablespace_BusinessSpace.sql file, available in the following location: *profile_root*/dbscripts/BusinessSpace/*node_name_server_name*/*database_type*/*database_name* for a stand-alone server, or *profile_root*/dbscripts/BusinessSpace/*cluster_name*/*database_type*/*database_name* for a cluster, where *database_type* is **DB2zOS**.

- Change the **VCAT** value from **@VCAT@** to the name or alias of the catalog of the integrated catalog facility for the storage group to use.

If you are using DB2 V9.x, and you would like performance improvements, edit the `createTablespace_BusinessSpace.sql` file. The `createTablespace_BusinessSpace.sql` file is available in *profile_root*`/dbscripts/BusinessSpace/`*node_name_server_name/database_type/database_name* for a stand-alone server, or *profile_root*`/dbscripts/BusinessSpace/`*cluster_name/database_type/database_name* for a cluster.

- Change **IMMEDIATE SIZE 8000 PAGESIZE 32K** to **IMMEDIATE SIZE 8000 AUTOMATIC PAGESIZE 32K**.
- Add the line **PREFETCHSIZE AUTOMATIC** after **EXTENTSIZE 16** under both **CREATE SYSTEM TEMPORARY TABLESPACE @TSDIR@TMPTP** and **CREATE REGULAR TABLESPACE @TSDIR@REGTP**.

The `configBusinessSpaceDB` script sets up tables for Business Space with a specific database. (If you want to create tables on an existing database other than the specific one, use the `createDBTables` script with your product instead of the `configBusinessSpaceDB` script.)

**Important:** Business Space tables must be created in a table space with a page size of 32K. If the default table space does not have a page size of 32K, the tables are not created.

To configure the database tables for Business Space, complete the following steps:

1. Make sure that you are using a user ID with sufficient authority to create tables.
2. Locate the script in the profile you most recently configured, and save it to a location on the same system with the database.
   - For all databases except DB2 for z/OS, locate the `configBusinessSpaceDB.bat` or `configBusinessSpaceDB.sh` script.
   - For DB2 for z/OS, if you do not run the `createDB.sh` script, you must run the Business Space files individually. Locate `createTablespace_BusinessSpace.sql` and `createTable_BusinessSpace.sql`.

   By default, the scripts are located in the following directory: *profile_root*`/dbscripts/BusinessSpace/`*node_name_server_name/database_type/database_name* for a stand-alone server, or *profile_root*`/dbscripts/BusinessSpace/`*cluster_name/database_type/database_name* for a cluster. The updated scripts (with the information that you entered during profile creation) are located in the profile for the server or cluster that you most recently configured. If you used the Deployment Environment Configuration wizard, the scripts are located in the deployment manager profile. When you configure a remote database, copy the scripts from the system where your product is installed to a place on the remote system.
3. Edit the script from step 2, and change the page size to 32K.
4. Open a command prompt and run one of the following commands, based on your operating system.

   Copy the folder with the batch files and scripts to the same location as your database and run the command there. Your user ID must have access to the command-line interpreter for the database type and have permission to run commands.

   - Linux UNIX `configBusinessSpaceDB.sh`
   - Windows `configBusinessSpaceDB.bat`

   For DB2 and SQL Server, use the optional **-createDB** parameter if you want to create a different database instead of using the existing database.

   **Restriction:** When using SQL Server, you see the following warning statements in the `systemout.log` file after running the database script: **... Warning! The maximum key length is 900 bytes ...**. If you are using the federated repositories as a user registry, you can ignore the warnings. If you are using the stand-alone LDAP registry, ensure that the number of characters in all the user distinguished name

(DN) entries in your organization do not exceed the 131 character limit. If the number of characters in any of the user DN entries exceeds 131 characters, you must change the user account registry to the federated repositories option.

For DB2 for z/OS, run the following files in order:

- `createTablespace_BusinessSpace.sql`
- `createTable_BusinessSpace.sql`

5. Linux UNIX Windows For DB2 and DB2 for z/OS, bind the command-line interface to the Business Space database using the following commands:

   **db2 connect to *database_name***

   **db2 bind *DB2_installation_directory*\bnd\@db2cli.lst blocking all grant public**

   **db2 connect reset**

   where:

   *database_name* is the name of the Business Space database

   *DB2_installation_directory* is the directory where DB2 is installed

6. If you are creating the Business Space database again, after it had been previously deleted, you must import the Business Space templates and spaces before you can use the Business Space environment. Complete the steps at Updating Business Space templates and spaces after installing or updating widgets.

- Update the endpoints for widgets that you want to be available in Business Space.
- Set up security for Business Space and the widgets that your team is using.

**Registering Business Space widget REST service endpoints using the command line:**

If you configure Business Space using the administrative console, you must register Representational State Transfer (REST) endpoints so that your team can use the widgets in Business Space. If you do not register your endpoints on the administrative console using the Business Space Configuration and the System REST service endpoint registration pages, you can use the **registerRESTServiceEndpoint** command.

Before you complete this task, you must complete the following tasks:

- Install the product.
- Configure the REST services for the widgets that you are you using in Business Space by using the REST Services administrative console page or the **updateRESTGatewayService** command. If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, the REST services are configured and enabled automatically.
- Configure Business Space by using either the Business Space Configuration administrative console page or the **installBusinessSpace** and **configureBusinessSpace** commands.
- Configure the database tables (if you are using a remote database or a network deployment environment).

REST services are registered automatically if you have a stand-alone server environment and you configured Business Space with the administrative console or the Profile Management Tool, or if you used the Deployment Environment wizard to configure your runtime environment. Otherwise, you must configure the REST services and then register them.

You can use the System REST service endpoint registration administrative console page or the **registerRESTServiceEndpoint** command to register endpoints for REST services for all of your product's widgets in Business Space. Then Business Space automatically associates widgets with these endpoints, and the widgets appear in the Business Space palette for use.

You can use the **registerRESTServiceEndpoint** command to register a set of endpoints for a given provider, a deployment target, or all unique endpoints in a cell. This command registers the endpoints of the REST services that are in the same cell as Business Space.

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.
2. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
3. Use the **registerRESTServiceEndpoint** command to register the Business Space endpoints for REST services for all your product's widgets.
4. After each command, run the save command.

The following example uses Jython to run the **registerRESTServiceEndpoint** command and then save the changes. It registers all configured and enabled REST services on the cluster with Business Space.

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster]')
AdminConfig.save()
```

where *name_of_rest_services_cluster* is the cluster name where REST services are configured and *name_of_business_space_cluster* is the cluster name where Business Space is deployed.

The following example uses Jacl:

```
$AdminTask registerRESTServiceEndpoint
{-clusterName name_of_rest_services_cluster
-businessSpaceClusterName name_of_business_space_cluster}
$AdminConfig save
```

where *name_of_rest_services_cluster* is the cluster name where REST services are configured and *name_of_business_space_cluster* is the cluster name where Business Space is deployed.

The **appName**, **webModuleName**, **type**, **name**, **version**, **nodeName**, **serverName**, or **clusterName** parameters are optional.

If you do not specify **type**, **appName**, and **webModuleName** parameters, all unique REST service endpoints configured on the deployment target are registered.

If you do not specify any of those parameters, all unique REST service endpoints configured on any deployment target are registered.

**Tip:** Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. For more information, see Changing the timeout settings for the Business Space Ajax proxy.

**Removing the virtual host from the primary cluster member:**

In some network deployment topologies, administrators might remove the virtual host from the primary member of a cluster to ensure that all traffic goes through a web server. Configuring Business Space on a cluster restores the virtual host, and you might decide to remove the virtual host so that your environment works the same way that it was set up originally.

Business Space requires one cluster member to perform load operations for the initial startup of the server. If the primary cluster member does not have a virtual host, the Business Space configuration adds a virtual host to perform the initial load operations.

After you have configured Business Space on a cluster, check the WebSphere Application Server ***default_host*** list to see whether it contains a virtual host for the primary cluster member.

To remove access to the virtual host, complete one of the following actions.

- Disable the virtual host for the primary cluster member after the initial startup of the cluster.
- Delete the virtual host for the primary cluster member using the administrative console (click **Environment** > **Virtual Hosts** > ***default_host*** > **Host Aliases**) or commands (see Working with virtual host properties files in the WebSphere Application Server documentation).

**Configuring a proxy server or load-balancing server to use with Business Space:**

If you are using Business Space in an environment with a proxy server or a load-balancing server, you must set up your environment so that Business Space and widgets work properly.

In a Network Deployment, or clustered, environment, you might set up a proxy server or an HTTP server for routing, security reasons, and for workload balancing. Instead of incoming HTTP requests going directly to an application server, they go to a proxy server that can spread the requests across multiple application servers that perform the work.

You can use other routing servers in place of or in front of the proxy server, for example IBM HTTP Server.

**Important:** The proxy server (or an alternate routing server) is required for workload balancing HTTP requests across two or more cluster members. The proxy server allows clients to access the applications within this topology.

In an environment with a load-balancing server or a proxy server between the browser and the Business Space and REST services, make sure that what you designate for the REST services protocol, host, and port matches the browser URL for accessing Business Space. On the REST service providers page on the administrative console, verify that for all providers, such as the Business Flow Manager and the Human Task Manager, have the correct protocol, host, and port. For more information about modifying the REST services, see Configuring REST services in a service provider.

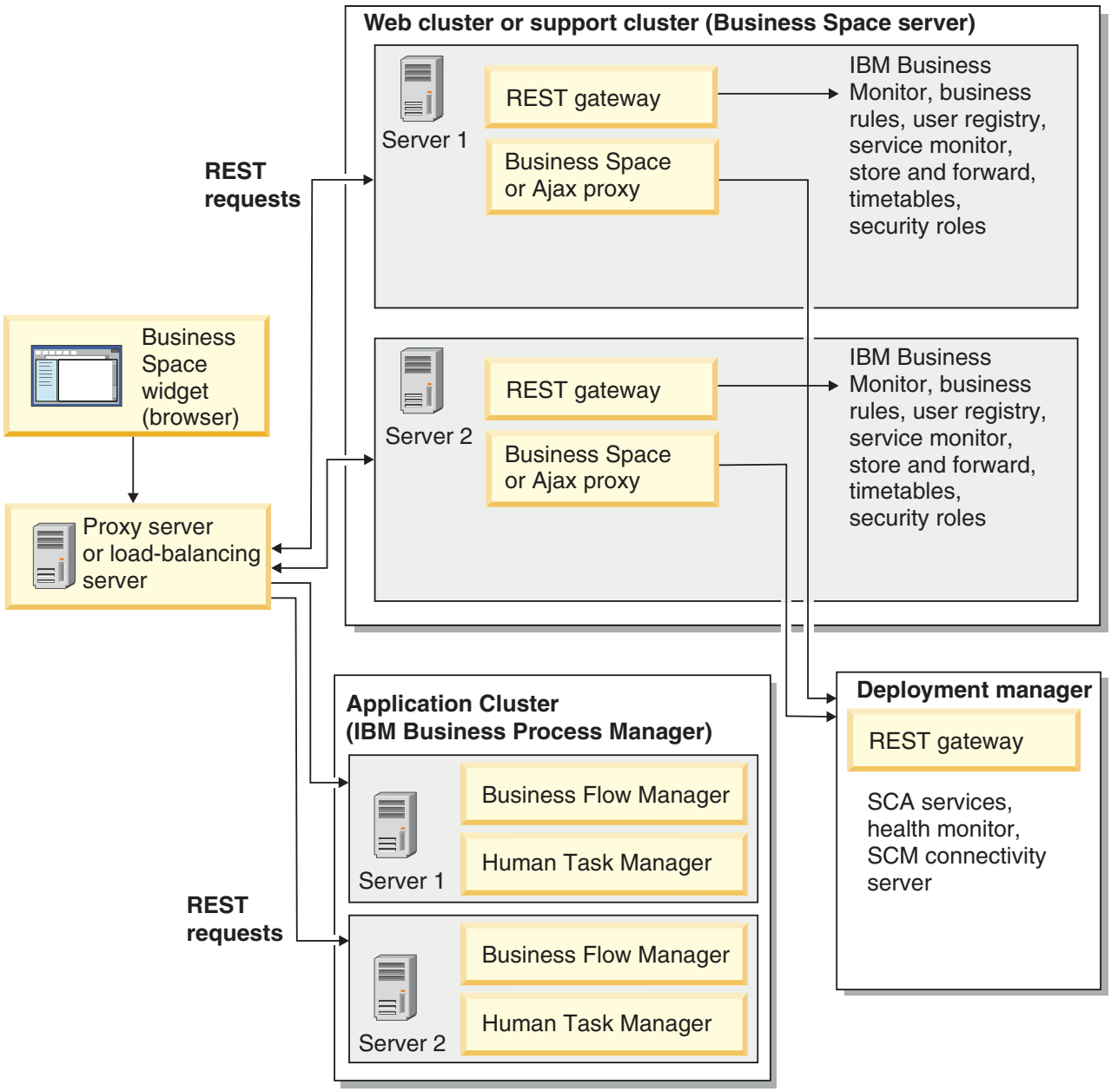



*Figure 1. Typical topology*

If you use IBM HTTP Server, you must complete additional mapping steps to verify that modules are mapped to the web server and that the host aliases are configured.

If you use a WebSphere Application Server proxy server, you must make sure that all the modules are enabled for the proxy server.

If you use a reverse proxy setup for an HTTP server, you must map the URLs for Business Space and widgets.

*Configuring IBM HTTP Server for Business Space:*

If you use IBM HTTP Server, you must complete additional mapping steps so that Business Space works in your environment.

Before you configure IBM HTTP Server to work with Business Space, complete the following steps:

- Install IBM HTTP Server
- Make sure that Secure Sockets Layer (SSL) is enabled for IBM HTTP Server.
- Make sure that the web server definition for IBM HTTP Server has been added to the application server.

  During the installation of the IBM HTTP Server plug-in, a `configure`*`Web_server`* script is produced by the installation process on the web server machine. The `configure`*`Web_server`* script is intended to map web application modules to the web server. Therefore, run this script after the generation of the deployment environment.

1. Make sure that modules are mapped to the web server. For each of the applications required by Business Space, verify that the web server is one of the selected targets.
   a. Log in to the administrative console as an administrative user.
   b. Click **Applications** > **Application Types** > **WebSphere enterprise applications**.
   c. From the Enterprise Applications panel, click the name of the application.

      Check the following applications. You might have some or all applications in this list, based on which products you are using with Business Space.

      - For all products.
        - **BSpaceEAR**_*nodename_servername*
        - **BSpaceForms**_*nodename_servername*
        - **BSpaceHelp**_*nodename_servername*
        - **BusinessSpaceHelpEAR**_*nodename_servername*
        - **REST Services Gateway**
        - **mm.was**_*nodename_servername*
        - **PageBuilder2**_*nodename_servername*
      - For IBM Business Process Manager.
        - **BPCExplorer**_*nodename_servername* (only for IBM BPM Advanced)
        - **BPEContainer**_*nodename_servername* (only for IBM BPM Advanced)
        - **BPMAdministrationWidgets**_*nodename_servername* (only for IBM BPM Advanced)
        - **HumanTaskManagementWidgets**_*nodename_servername* (only for IBM BPM Advanced)
        - **IBM_BPM_Help**_*nodename_servername*
        - **IBM_BPM_PerformanceDW**_*nodename_servername*
        - **IBM_BPM_Portal**_*nodename_servername*
        - **IBM_BPM_ProcessAdmin**_*nodename_servername*
        - **IBM_BPM_Process_Portal_Notification**_*nodename_servername*
        - **IBM_BPM_Process_Portal**_*nodename_servername*
        - **IBM_BPM_Repository**_*nodename_servername* (only for Process Center)
        - **IBM_BPM_Teamworks**_*nodename_servername*
        - **IBM_BPM_WebAPI**_*nodename_servername*
        - **REST Services Gateway Dmgr** (only for IBM BPM Advanced)
        - **TaskContainer**_*nodename_servername* (only for IBM BPM Advanced)
      - For WebSphere Enterprise Service Bus.
        - **BPMAdministrationWidgets**_*nodename_servername*
        - **REST Services Gateway Dmgr**
        - **wesbWidgets**_*nodename_servername*
      - For IBM Business Monitor.
        - **HumanTaskManagementWidgets**_*nodename_servername*

– **WBMDashboardWeb_*nodename_servername***

d. For each application, on the Configuration tab, under Modules, click **Manage Modules**.

e. On the Manage Modules page for your application, make sure that the web server is one of the selected targets for each of your modules.

- In the table, check the Server column for each module to make sure that the web server is one of the selected targets for each of your modules. For example, for the mm.was_*nodename_servername* application, look for the web server to be displayed in the Server column: **WebSphere:cell=qaxs41Cell02,node=qaxs41Node03,server=httpserver WebSphere:cell=qaxs41Cell02,cluster=Golden.WebApp**.
- If you need to add the web server, select the check box next to the name of the module. Then, in the Clusters and servers list, use the Ctrl key to select multiple targets. For example, to have a web server serve your application, press the Ctrl key and then select the application server cluster and the web server together. Click **Apply**, **OK** and **Save** to save any changes.

2. Verify that the host name alias `default_host` contains the correct information for every cluster member, web server, or proxy server.

a. Log in to the administrative console as an administrative user.

b. Click **Servers** > **Server Types** > **WebSphere application servers**.

c. For every cluster member, click the name of the application server to view the port number for the **WC_defaulthost** port name.

- Under Communications, expand **Ports**.
- For the port name **WC_defaulthost**, remember its port number.

d. From the left navigation area of the administrative console, click **Environment** > **Virtual hosts**.

e. Click the **default_host** name.

f. Under Additional Properties, click **Host Aliases**.

g. If the host name and port number for the cluster members is not displayed on the list, click **New** to add the missing entry to the list. The wildcard character * (asterisk) is supported for the host name.

h. If you add a new entry, click **Save** and **Synchronize**.

3. When using an HTTP server front end to work with Business Space, you must set **Accept content for all requests** to **true** for the web server plug-in in the WebSphere Application Server administrative console under **Web servers** > **webserver1** > **Plug-in properties** > **Request and response**.

*Configuring a WebSphere Application Server proxy server for Business Space:*

If you use a WebSphere Application Server proxy server, make sure that all the modules are enabled for the proxy server so that Business Space works in your environment.

Before you configure WebSphere Application Server proxy server to work with Business Space, complete the following steps:

1. Make sure that you have applied the latest version of WebSphere Application Server.
2. Create a proxy server (click **Servers** > **Server Types** > **WebSphere proxy servers**). For more information, see Setting up the proxy server in the WebSphere Application Server information center.
3. Make sure that the HTTP protocol is selected.

1. Optional: Make sure that modules are mapped to the WebSphere Application Server proxy server. For each of the applications that Business Space requires, verify that the modules are enabled for the proxy server.

a. Log on to the administrative console as an administrative user.

b. Select **Applications** > **Application Types** > **WebSphere enterprise applications**.

c. From the Enterprise Applications panel, select the name of the application.

Check the following applications. You might have some or all applications in this list, based on which products you are using with Business Space.

- For all products.
  - **BSpaceEAR**_nodename_servername_
  - **BSpaceForms**_nodename_servername_
  - **BSpaceHelp**_nodename_servername_
  - **BusinessSpaceHelpEAR**_nodename_servername_
  - **REST Services Gateway**
  - **mm.was**_nodename_servername_
  - **PageBuilder2**_nodename_servername_
- For IBM Business Process Manager.
  - **BPCExplorer**_nodename_servername_ (only for IBM BPM Advanced)
  - **BPEContainer**_nodename_servername_ (only for IBM BPM Advanced)
  - **BPMAdministrationWidgets**_nodename_servername_ (only for IBM BPM Advanced)
  - **HumanTaskManagementWidgets**_nodename_servername_ (only for IBM BPM Advanced)
  - **IBM_BPM_Help**_nodename_servername_
  - **IBM_BPM_PerformanceDW**_nodename_servername_
  - **IBM_BPM_Portal**_nodename_servername_
  - **IBM_BPM_ProcessAdmin**_nodename_servername_
  - **IBM_BPM_Process_Portal_Notification**_nodename_servername_
  - **IBM_BPM_Process_Portal**_nodename_servername_
  - **IBM_BPM_Repository**_nodename_servername_ (only for Process Center)
  - **IBM_BPM_Teamworks**_nodename_servername_
  - **IBM_BPM_WebAPI**_nodename_servername_
  - **REST Services Gateway Dmgr** (only for IBM BPM Advanced)
  - **TaskContainer**_nodename_servername_ (only for IBM BPM Advanced)
- For WebSphere Enterprise Service Bus.
  - **BPMAdministrationWidgets**_nodename_servername_
  - **REST Services Gateway Dmgr**
  - **wesbWidgets**_nodename_servername_
- For IBM Business Monitor.
  - **HumanTaskManagementWidgets**_nodename_servername_
  - **WBMDashboardWeb**_nodename_servername_

d. For each application, if you click the name of the application, then **Virtual hosts**, verify that it uses the value **default_host**.

e. For each application, on the **Configuration** tab, under **Modules**, click **Manage Modules**, then on the Manage Modules page for the application, click each module, and select **Web Module Proxy Configuration** and verify that **Enable Proxy** is selected.

2. Verify that the host name alias `default_host` contains the correct information for every cluster member, web server, or proxy server.

a. Log on to the administrative console as an administrative user.

b. Select **Servers** > **Server Types** > **WebSphere application servers**.

c. For every cluster member, select the name of the application server to view the port number for the **WC_defaulthost** port name.

- Under Communications, expand **Ports**.
- Note the port number for the **WC_defaulthost** port.

d. From the left navigation area of the administrative console, select **Environment** > **Virtual hosts**.
e. Click **default_host**.
f. Under Additional Properties, click **Host Aliases**.
g. If the host name and port number for the cluster members is not displayed in the list, click **New** to add the missing entry to the list. You can use the wildcard character * (asterisk) for the host name.
h. If you add a new entry, click **Save** and then click **Synchronize**.

3. To use HTTP protocol, configure the WebSphere Application Server proxy server.
   a. Log on to the administrative console as an administrative user.
   b. Select **Servers** > **Server Types** > **WebSphere proxy servers**, and then select the proxy server that you previously created.
   c. Expand **HTTP Proxy Server Settings** and click **Proxy settings**.
   d. Click **Custom Properties** and add a new property with a name of `cache.query.string` for a name and a value of `true`.
   e. Click **Save**, and then restart the proxy server.

*Mapping Business Space URLs for a reverse proxy server:*

If you have a reverse proxy setup for your HTTP server, when you are configuring the HTTP server to work with Business Space, you must map the URLs for Business Space and the widgets that your team uses.

1. Edit your HTTP server configuration file.
2. Map all of the URLs for Business Space and the widgets that your business users work with in the runtime solution.

   URLs for general Business Space framework (all products):
   - /BusinessSpace/*
   - /mum/*
   - /BusinessSpaceHelp/*
   - /BSpaceWebformsProxy/*
   - /themes/*
   - /pageBuilder2/*

   Additional URLs for IBM Business Monitor widgets:
   - /BusinessDashboard/*
   - /monitorServerComponent/*
   - /mobile/*
   - /rest/*
   - /p2pd/*

   **Note:** The /p2pd/* URLs apply to IBM Cognos Business Intelligence.

   Additional URLs for IBM Business Process Manager Advanced widgets:
   - /BSpaceWidgetsHM/*
   - /SecurityManagerWidgets/*
   - /BSpaceWidgetsBCM/*
   - /rest/*
   - /ProcessPortal/*
   - /PolymorphicWidget/*
   - /scaWidget/*
   - /ServiceMonitorGraphWidget/*

- /StoreAndForward/*

Additional URL for IBM Business Process Manager Standard to work with Process Portal:

- /ProcessPortal/*

Additional URLs for WebSphere Enterprise Service Bus widgets:

- /BSpaceWidgetsHM/*
- /rest/*
- /PolymorphicWidget/*
- /scaWidget/*
- /ServiceMonitorGraphWidget/*
- /StoreAndForward/*

**Enabling the Federation API across multiple deployment targets:**

The Federation API allows you to display processes and tasks created in Process Designer and Integration Designer in the same task list. If your environment has multiple clusters in the same cell or includes multiple cells, you must manually configure the federation domains using commands.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Advanced
- IBM Business Process Manager Standard

Before you complete this task, you must complete the following tasks:

- Install the product.
- Create profiles, and configure Business Space on a deployment target (server or cluster).
- Configure the database tables (if you are using a remote database or deployment environment).

The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands.

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.
2. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
3. Use the **createBPMApiFederationDomain** command to create a federation domain, and use the **addTarget** step to federate the domain across one or more deployment targets.

   For the name parameter, the *federation_domain_name* must be unique.

   The following example adds a federation domain with name **myCustomFederationDomain** that federates across a server (with the node name **myNode** and server name **myServer**) and a cluster (with the name **myCluster**).

   - Jython example:

     **AdminTask.createBPMApiFederationDomain('[-nodeName** *node_name* **-serverName** *server_name* **-name myCustomFederationDomain -addTarget [["" myNode myServer ""] ["" "" "" myCluster]]]')**
   - Jacl example:

     **$AdminTask createBPMApiFederationDomain {-nodeName** *node_name* **-serverName** *server_name* **-name myCustomFederationDomain -addTarget {{"" myNode myServer ""} {"" "" "" myCluster}}}**

Other commands are available if you need to modify the Federation API configuration.

- If you want to delete a federation domain including the contained targets, use the **deleteBPMApiFederationDomain** command.

- If you want to list all federation domains, use the **listBPMApiFederationDomains** command.
- If you want to add or remove targets from a federation domain, use the **modifyBPMApiFederationDomain** command.
- If you want to display details about a federation domain, use the **showBPMApiFederationDomain** command.

**Enabling Business Space widgets for cross-cell environments:**

You must manually edit endpoints files if Business Space is running on a different cell than where the Representational State Transfer (REST) services are running, or if widgets are on different cells than Business Space.

Before you complete this task, you must have completed the following tasks:
- Installed the product.
- Created profiles, and configured Business Space on a deployment target (server or cluster).
- Configured the database tables (if you are using a remote database or deployment environment).

All widgets required for your product are installed with Business Space, but you must configure and register the endpoints needed by the widgets before your team can use them in Business Space. You can configure and register the endpoints by using administrative console pages. However, if your product and REST services are installed on a different cell than Business Space, you must edit REST service endpoints files so that they access the REST services and your widgets work properly in Business Space.

Edit one or more of the service endpoint files and widget endpoint files, based on the products you have installed, and the widgets you are using with Business Space. Service endpoint files typically contain `Endpoint` or `Endpoints` in the XML file name, and widget endpoint files typically contain `Widget` or `Widgets` in the XML file name. The following list includes IBM business process management examples of service endpoint files and widget endpoint files:
- IBM Business Monitor: `monitorEndpoints.xml` and `monitorWidget.xml`
- IBM Business Monitor with IBM Cognos Business Intelligence: `cognosEndpoints.xml` and `cognosWidget.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `bpmAdministrationEndpoints.xml` and `BPMAdministrationWidgetEndpoints.xml` (for Administration widgets)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` and `BPMAdministrationWidgetEndpoints.xml` (for Administration widgets), `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `HumanTaskManagementEndpoints.xml` (for business processes and human tasks), `bspaceWFSEndpoints.xml` (for using Lotus Webform Server with Human Task Management widgets)
- All products: `wsumEndpoint.xml` and `wsumWidget.xml` (for user membership)

If you are an administrator, you can register endpoints and enable widgets by performing the following steps.
1. Copy the remote widget compressed file found at *install_root*`\BusinessSpace\registryData\`*product_name*`\`*product_name_widget_set_name*`_crosscell.zip` to the cell where Business Space is configured during product installation. Widgets can be found in the directory and can be copied to a temporary folder.
2. Extract the `crosscell.zip` to a temporary directory.
3. Locate the service endpoint files and widget endpoints files.

   In the directory where you extracted the file, look in the `endpoints` directory to view all the widget endpoint files and service endpoint files. The file names typically end with `Endpoints.xml` or `Endpoint.xml`.

4. Configure the endpoints as needed by editing the service endpoint files and the widget endpoint files.
   a. Edit the service endpoint files to point to the service.

      Each endpoint in the service endpoint file is designated by a **<tns:Endpoint>** block. Identify the block that you want to change. Look for comments that identify where you make the edits, for example:

      ```
      <!-- When your REST service is remote from your Business Space server, update the following
      url value with the fully qualified URL to the service.
      For example https://host.domain.com:9443/rest/bpm/monitor/ -->
       <tns:url>/rest/bpm/monitor/</tns:url>
      ```

      **Tip:** If you do not intend to activate some endpoints, you can remove them from the file to prevent confusion.

      The location identified by an endpoint is specified in **<tns:url>**. This value is a path in a web module, specified as a full or relative HTTP URL. By default, the URL is relative. Change it to a full URL path, for example, **https://*virtualhost*.com:*virtualport*/rest/bpm/htm** or **http://host1:9445/WBPublishingDRAFT/**, where the protocol, host, and port identify how the product web module can be accessed.

      To locate the port number for the server, perform the following steps:

      - Log in to the administrative console.
      - Click **Servers** > **Server Types** > **WebSphere application servers**.
      - Click the server for which you want to find the port number, and then expand the Ports section.

      All applications use the same port as shown in either the **wc_defaulthost** (unsecured host) parameter or the **wc_defaulthost_secure** (secure host) parameter.

      **Tip:** If you are using an HTTP server to access your web modules for load balancing, use the host name and port settings of the HTTP server.
   b. Edit the widget endpoint files to point to the Business Space location where the widgets are deployed.

      Each endpoint in the service endpoint file is designated by a **<tns:id>** block. Identify the block that you want to change. Look for comments that identify where you make the edits, for example:

      ```
      <!--  When using widgets in a remote configuration, update the following
      url value with the fully qualified URL of the widget web module.
      For example https://host.domain.com:9443/BusinessDashboard/ -->
      <tns:url>/BusinessDashboard/</tns:url>
      ```

      The location identified by an endpoint is specified in **<tns:url>**. Change it to a full URL path that points to the Business Space location where the widgets are deployed, for example, **https://*host.domain*.com:*port*/BusinessDashboard/**
5. In the cell where the Business Space server is configured, run the **updateBusinessSpaceWidgets** command to update the endpoint URLs after you have modified the endpoints XML files.
   a. For your profile, open a command window. The wsadmin command can be found at the profiles*profile_name*\bin directory. For a clustered environment, run the command from the *deployment_manager_profile_root*\bin directory. For a stand-alone server environment, run the command from the *profile_root*\bin directory.
   b. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
   c. Run the **updateBusinessSpaceWidgets** command. For a clustered environment, specify the **-clusterName** parameter. For a stand-alone server environment, specify the **-serverName** and **-nodeName** parameters. Specify the **-endpoints** parameter with the full path for the directory where you extracted the widget endpoint files. Specify the **-catalogs** parameter to point to the directory where you extracted the widget catalog file.
6. Restart the server.

The following example endpoint file is for IBM Business Monitor widgets.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- START NON-TRANSLATABLE -->
<tns:BusinessSpaceRegistry
 xmlns:tns="http://com.ibm.bspace/BusinessSpaceRegistry"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
 BusinessSpaceRegistry.xsd ">

  <tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Location of backing services for Monitor widgets
</tns:description>
  </tns:Endpoint>

</tns:BusinessSpaceRegistry>
<!-- END NON-TRANSLATABLE -->
```

- After running the **installBusinessSpaceWidgets** command or the **updateBusinessSpaceWidgets** command, you must perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.
- For multiple instances of service endpoints, for example for partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster. You must edit both the widget endpoints files and the widget catalog files. For more information, see Enabling Business Space widgets to work with multiple endpoints.
- If you have enabled security for your environment, you must make sure that it is set up properly to work with Business Space.

**Enabling Business Space widgets to work with multiple endpoints:**

If you have one Business Space instance configured and you have a need to create another instance of the service endpoints in your environment, you must configure Business Space so that the widgets can display data from the multiple service endpoints. You must edit two files: the endpoints file, which registers endpoints with Business Space, and the widget catalog file, which contains definitions of widgets.

Before you complete this task, you must have completed the following tasks:

- Installed the product.
- Created a server or cluster and configured it for Business Space .
- Configured the database tables (if you are using a remote database or deployment environment).
- Configured the additional Representational State Transfer (REST) services for your additional widgets.

In a deployment environment, you can have partitioning of work. For example, you can have two clusters, one that processes accounting data and one that processes insurance data. However, a service endpoint serves only one cluster. To access both partitions of work from Business Space, you must register two separate widgets, one for each partition of work, so you can access them both from Business Space. For example, you could have an Account Human Task List widget and an Insurance Task List widget in the catalog (both with the same actual human task list code).

You must manually edit the endpoints file and the widget catalog file.

Widget service endpoint files are bundled with each product and are added during the installation of the product. You must edit one or more service endpoint files, based on the products you have installed, and the widgets you are using with Business Space. The following list includes IBM business process management examples of widget service endpoint files:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor with IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `bpmAdministrationEndpoints.xml` (for Administration widgets)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (for Administration widgets), `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `HumanTaskManagementEndpoints.xml` (for business processes and human tasks), `bspaceWFSEndpoints.xml` (for using Lotus Webform Server with Human Task Management widgets)
- All products: `wsumEndpoint.xml` (for user membership)

Widget catalog files contain the definition of widgets for your product. You must edit one or more of the following widget files, based on the products you have installed, and the widgets you are using with Business Space. The following list includes IBM business process management examples of widget catalog files:

- IBM Business Monitor: `catalog_WBMonitor.xml`
- WebSphere Enterprise Service Bus: `catalogProxyGateway.xml` and `catalog_ServiceAdmin.xml`
- IBM Business Process Manager: `catalog_BPMAdministration.xml`, `catalog_BusinessRules.xml`, `catalog_ServiceAdmin.xml`, and `catalog_HumanTaskManagement.xml`

Both the service endpoint files and the widget catalog files are located at *install_root*`\BusinessSpace\registryData\`*product_name*`\`. The endpoints files are located in the `endpoints` subdirectory, and the catalog files are located in the `catalogs` subdirectory.

The*install_root*`\BusinessSpace\registryData\`*product_name*`\` directory contains service endpoint and widget catalog template files for your product. You can copy the files that you need to use as a template and add your changes.

1. In order to have multiple instances of a widget, you must install the applications that provide widgets with a unique application name and context root for each widget instance.
   a. Deploy the widget application on the Business Space deployment target (the same server or cluster on which the **BSpaceEAR_*server_node*** application is running) for each widget instance. The following list includes IBM business process management examples of widget Enterprise Archive (EAR) files:
      - BPMAdministrationWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus and IBM Business Process Manager)
      - HumanTaskManagementWidgets_*nodename_servername* (for IBM Business Process Manager and IBM Business Monitor)
      - WBMDashboardWeb_*nodename_servername* (for IBM Business Monitor)
      - wesbWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus)
   b. When deploying, update the application name and the web module context root names to a unique name. Take note of the context root names that you use.
2. Edit the new REST service endpoints for the additional application deployment targets (the server or cluster where the REST services application is deployed). Create a service endpoints file to add service endpoints.
   a. Locate the endpoint files in the *install_root*`\BusinessSpace\registryData\`*product_name*`\endpoints` directory. Copy the endpoints template file, and remove all the endpoints that you do not intend to change.

b. Edit the endpoints file and add an additional service endpoint starting with **<tns:Endpoint>**, with a unique ID (**<tns:id>**) and the URL for the new endpoint (**<tns:url>**), but with the same version, and optionally all the locales as the original endpoint. The type (**<tns:type>**) must have the same value as the ID (**<tns:id>**). You can change the name and description, for example, **My team's insurance task list**.

c. When adding endpoints, pay attention to the following information:

- **<tns:id>**: The ID can be any string but must be unique for all registered endpoints. Ensure that this ID is unique when you are adding additional endpoints.
- **<tns:type>**: The type must have the same value as **<tns:id>**.
- **<tns:url>**: For the service endpoint, if the URL is relative, then it is assumed that the REST service endpoint is co-located with the Business Space server. If the URL is relative, make sure the URL is same as the context root you deployed, but with beginning and end directory indications, for example, **<tns:url>/REST_Endpoint_for_server2/</tns:url>**. If your endpoint is on a remote system, update this field with an absolute URL, but with an end directory indication.
- **<tns:description>**: Type a meaningful description that further details the nature of the data set that this endpoint is working on. It could either be based on the cluster that is working on the data set or the nature of the data set, for example, **insurance claim human tasks** or **accounting data human tasks**.

d. Save your changes.

Example service endpoint, located in `monitorEndpoints.xml`:

```
<tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/bpm/monitor/</tns:url>
    <tns:description>Location of backing services for Monitor widgets
</tns:description>
  </tns:Endpoint>
```

3. In the service endpoints file, add a widget endpoint for each widget instance.

a. Edit the endpoints file that you created in step 2. Add an additional widget endpoint starting with **<tns:Endpoint>** and with a unique ID (**<tns:id>**). The type (**<tns:type>**) must have the same value as the ID (**<tns:id>**). The URL for the new endpoint (**<tns:url>**) should be the same as the context root you deployed in step 1., but with beginning and end directory indications, for example, **<tns:url>/BSpaceWidgetsWPS2/</tns:url>**. The widget endpoint you add should contain the same version and can optionally contain all the locales as the original endpoint. You can change the name and description.

b. When adding endpoints, pay attention to the following information:

- **<tns:id>**: The ID can be any string but must be unique for all registered endpoints. Ensure that this ID is unique when you are adding additional endpoints.
- **<tns:type>**: The type must have the same value as **<tns:id>**.
- **<tns:url>**: For the widget endpoint, make sure the URL is same as the context root you deployed, but with beginning and end directory indications, for example, **<tns:url>/ BSpaceWidgetsWPS2/</tns:url>**.
- **<tns:description>**: Type a meaningful description that further details the nature of the data set that this endpoint is working on. It could either be based on the cluster that is working on the data set or the nature of the data set, for example, **insurance claim human tasks** or **accounting data human tasks**.

c. Save your changes.

Example widget endpoint, located in `monitorEndpoints.xml`:

```
<tns:Endpoint>
<tns:id>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:type>
```

```
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/BusinessDashboards/</tns:url>
    <tns:description>Location for Monitor widgets</tns:description>
  </tns:Endpoint>
```

4. Create a widget catalog file to add new widget definitions.
   a. Locate the widget catalog file in the *install_root*\BusinessSpace\registryData*product_name*\catalogs directory. Copy the catalog template file. For the new file name, use the following standard: catalog_*widget*.xml (with no spaces in the file name), where *widget* is the same as the id value of the **<catalog>** element in the file. Remove all the **<category>** elements that you do not intend to change. For the category that you are working with, remove all the **<entry>** elements that you do not intend to change.
   b. Add an **<entry>** with a unique ID, for example, **id="{com.ibm.bspace.widget}***widget_id* and a unique name, for example, **unique-name="{com.ibm.bspace.widget}***widget_name*. You can keep all the other definitions.
   c. Change the title and description to make the new widget available as a distinct widget in Business Space that outlines the nature of the new endpoint. For example, you could name your widget **My team's insurance task list** in the **<title>**. The title should help the business users choose the right widget. The description should help the business users understand the nature of the data and the functionality of the widget that they are selecting.
   d. Edit the new widget catalog XML file to reference the new widget endpoint: Change the definition to match the **<tns:id>** of the widget endpoint you added in step 3.a.

      For example, change it to: **...**

      **<definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId2/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>**

      **...**
   e. In the **<metadata>** of the catalog file, make sure the **endpoint://** matches the type and the ID in the endpoint file (**<tns:type>** and **<tns:id>**).
   f. In the **<metadata>** of the catalog file, make sure the **"refVersion" :** matches the version in the endpoint file (**<tns:version>**).
   g. Save your changes.

   You can use the widget definition in the example code snippet below as a basis to make your changes::

```
<entry id="{com.ibm.wbimonitor}instances"
unique-name="{com.ibm.wbimonitor}instances">
            <title>
                <!-- END NON-TRANSLATABLE -->
                <nls-string xml:lang="en">Instances</nls-string>
                <!-- START NON-TRANSLATABLE -->
            </title>
            <description>
                <!-- END NON-TRANSLATABLE -->
                <nls-string xml:lang="en">Instances</nls-string>
                <!-- START NON-TRANSLATABLE -->
            </description>
        <shortDescription>
                    <!-- END NON-TRANSLATABLE -->
              <nls-string xml:lang="en">This widget displays a dashboard with
the available monitoring context in either individual instances or user-
defined groups of context instances.</nls-string>
                    <!-- START NON-TRANSLATABLE -->
            </shortDescription>
            <definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId
/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
            <content>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
thumb_instances.gif</content>
            <preview>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
prev_instances.gif</preview>
```

```
   <previewThumbnail>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/
img/prev_instances.gif</previewThumbnail>
   <help>endpoint://{com.ibm.bspace}bspaceWidgetHelpRootId/topic/
com.ibm.bspace.help.widg.mon.doc/topics/help_instance_whatis.html</help>
            <icon>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
icon_instances.gif</icon>
   <metadata name="com.ibm.mashups.builder.autoWiringEnabled">true
</metadata>
            <metadata name="com.ibm.bspace.version">7.0.0.0</metadata>
            <metadata name="com.ibm.bspace.owner">International Business
Machines Corp.</metadata>
            <metadata name="com.ibm.bspace.serviceEndpointRefs">
[{"name":"serviceUrlRoot", "required":"true",
"refId":"endpoint://{com.ibm.wbimonitor}monitorServiceRootId",
"refVersion":"1.0.0.0"}]</metadata>
        </entry>
```

5. Place the new service endpoint file and the new widget catalog file in a compressed file, and run the **updateBusinessSpaceWidgets** command, using the **-widgets** parameter to specify the compressed file location.

- After running the **updateBusinessSpaceWidgets** command, you must perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.
- If Business Space is running on a different cell than where the REST services are running, you must manually edit the endpoints files.
- If you have enabled security for your environment, you must make sure that it is set up properly to work with Business Space.

**Configuring widgets for multiple products:**

You can configure or add Business Space widgets for one product on a Business Space that has already been configured with a different product by using the **installBusinessSpaceWidgets** command.

Before you complete this task, you must complete the following tasks:

- Complete all steps to install and configure a product, and configure Business Space.
- Complete all steps to install and configure the additional product.

You can install more than one product that works with Business Space and configure the widgets for both products after you install the second product. However, if you install a second product after you have already configured Business Space with widgets for the first product, you must use the **installBusinessSpaceWidgets** command to add and configure the second product widgets to work with the same Business Space.

In a stand-alone augmentation, widgets are installed automatically. For example, widgets are installed if you create a stand-alone IBM Business Process Manager profile, configure the server for Business Space, install IBM Business Monitor, and augment the already-configured server to IBM Business Monitor.

1. Make sure the deployment manager profile is up and running, and on that profile, open a command window.

   The wsadmin command can be found at the `profiles/`*profile_name*`/bin` directory.
2. At the command prompt, type the **wsadmin** command to start the **wsadmin** environment.
3. Use the **installBusinessSpaceWidgets** command to install, deploy, and register designated widgets located in the *install_root*`/BusinessSpace/registryData/`*product_name*`/widgets` directory.

The following example uses Jython to run the **installBusinessSpaceWidgets** to install widgets for IBM IBM Business Monitor to work with the Business Space environment that has been previously configured for IBM IBM Business Process Manager.

```
AdminTask.installBusinessSpaceWidgets('[-nodeName node_name
 -serverName server_name -widgets
 install_root/BusinessSpace/registryData/WBM/widgets/Widgets_WBMonitor.zip]')
```

The following example uses Jacl:

```
$AdminTask installBusinessSpaceWidgets {-nodeName node_name
 -serverName server_name -widgets
 install_root/BusinessSpace/registryData/WBM/widgets/prWidgets_WBMonitor.zip}
```

After configuring the widgets, to enable Business Space for your runtime environment, you must perform the following steps.

- After running the **installBusinessSpaceWidgets** command or the **updateBusinessSpaceWidgets** command, perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.
- Configure REST services. For more information, see Configuring REST services.
- Register REST endpoints. For more information, see "Configuring Business Space and registering REST endpoints on the administrative console."
- Verify security is set up properly to work with Business Space and the widgets your team is using. For more information, see Setting up security for Business Space.

## Setting up specific widgets to work in Business Space

Some of the widgets that come with your product require additional configuration steps before you can use them in Business Space.

Your business process management product includes several widgets, and some require additional configuration to communicate with your solution from Business Space.

**Configuring the service monitor:**

If you are creating a new server and you want to use the Service Monitor widget in Business Space to measure the response time and request throughput for services exposed or invoked by an SCA module, configure and enable service monitoring in the administrative console.

**Required security role for this task**: If administrative security is enabled, you must be logged in with an administrative role to perform this task.

The service monitor server must be enabled before you can use the Service Monitor widget. In stand-alone server environments, the service monitor server is enabled by default during profile creation. In deployment environments and for new servers created using the administrative console, you must enable the service monitor server manually from the administrative console. For Remote Message and Remote Support topology patterns, the service monitor server must be enabled in the Support cluster, and for Remote Messaging, Remote Support, and Web (four-cluster) patterns the server must be enabled in the Web cluster.

The service monitor has a client/server architecture.

- Service monitor agent: Measures the throughput and response time for operations and sends the measurement data to the service monitor server
- Service monitor server: Gathers and aggregates response time and throughput measurements from all running service monitor agents, and then calculates and stores the statistics.

**Important:** If you are using an external HTTP server to access Business space, make sure to configure the HTTP server to allow encoded slashes. Refer to the HTTP server documentation for details.

1. Log into the administrative console with administrator privileges.
2. Configure the service monitor server.

a. From within the console, click **Servers** > **Server Types** > **WebSphere application servers** > *servername* > **Service Monitor**.
b. On the Service Monitor page, click **Enable service monitor**.
c. Examine the default values for the service monitor buffer size and the query size limit and, if necessary, revise them.
d. Specify the service monitoring targets. These are the service monitor agents you want to gather data from.

*Table 7. Monitoring*

| Targets to monitor | Steps to perform |
|---|---|
| Monitor all running service monitor agents | Ensure the **Enable all service monitor agents** option is checked. |
| Monitor a specific subset of running service monitor agents | 1. Clear the **Enable all service monitor agents** option. A collection table appears; if this is a new configuration, the table is empty.<br>2. Click **Add**. The Browse Deployment Targets page opens.<br>3. From the collection table on the Browse Deployment Targets page, select the deployment target whose agent you want to monitor.<br>4. Click **OK** to return to the Service Monitor Server page.<br>5. Repeat Step 2 through Step 4 until you have added all the agents you want to monitor. |

e. From the Service Monitor Server page, click **OK**. The configuration is saved and takes effect immediately.

3. Configure the service monitor agent.
   a. From within the console, click **Servers** > **Server Types** > **WebSphere application servers** > *servername* > **Service Monitor Agent**.
   b. On the Service Monitor Agent page, click **Enable service monitor agent**.
   c. Examine the default values for the agent configuration and, if necessary, revise them.
   d. Click **OK**.

**Installing the default business space on z/OS:**

In most operating systems, the default business space is installed automatically. However, for z/OS systems that are using the local OS user registry and SAF authorization, there are some extra steps that you must do to install the default business space.

Business Space uses the primary administrative user name for setting the administrator for the welcome space. However, on z/OS there is no concept of primary administrator when using the local OS user registry and SAF authorization. This means that you must provide a valid ID in the registry to install the default space.

- For a stand-alone server:
  1. Modify the **MashupAdminForOOBSpace** property in the configuration file `profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/config/ConfigService.properties` with a valid user ID.
  2. Run the command **updatePropertyConfig** in the wsadmin environment of the profile:
     – For Jython:

```
AdminTask.updatePropertyConfig('{-serverName server_name -nodeName node_name -propertyFileName
"profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/config/
ConfigService.properties"
-prefix "Mashups_"}')
```

– For Jacl:

```
$AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name -propertyFileName
"profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/config/
ConfigService.properties"
-prefix "Mashups_"}
```

3. Save your changes to the master configuration using one of the following commands:
   – For Jython:

   ```
   AdminConfig.save()
   ```

   – For Jacl:

   ```
   $AdminConfig save
   ```

   .
4. In the profile where the server is located, open the `profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/public/oobLoadedStatus.properties` file and update the **importSpaces.txt** property:

   ```
   importSpaces.txt=true
   ```

5. Restart the server.

- For a cluster:
  1. Modify the **MashupAdminForOOBSpace** property in the configuration file `deployment_manager_profile_root/BusinessSpace/cluster_name/mm.runtime.prof/config/ConfigService.properties` with a valid user ID.
  2. Run the command **updatePropertyConfig** in the wsadmin environment of the deployment manager profile:
     – For Jython:

     ```
     AdminTask.updatePropertyConfig('{-clusterName cluster_name -propertyFileName
     "profile_root/BusinessSpace/cluster_name/mm.runtime.prof/config/ConfigService.properties"
     -prefix "Mashups_"}')
     ```

     – For Jacl:

     ```
     $AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
     "profile_root/BusinessSpace/cluster_name/mm.runtime.prof/config/ConfigService.properties"
     -prefix "Mashups_"}
     ```

  3. Save your changes to the master configuration using one of the following commands:
     – For Jython:

     ```
     AdminConfig.save()
     ```

     – For Jacl:

     ```
     $AdminConfig save
     ```

     .
  4. Get the name of the cell, node, and server for the custom profile:
     a. In the deployment manager profile, open the `deployment_manager_profile_root/BusinessSpace/cluster_name/mm.runtime.prof/config/ConfigService.properties` file.
     b. Look for the name of the cell, node, and server in the **com.ibm.mashups.directory.templates** or **com.ibm.mashups.directory.spaces** properties.
     c. Use the name of the cell, node, and server to locate the custom profile.
  5. In the custom profile, open the `custom_profile_root/BusinessSpace/cluster_name/mm.runtime.prof/public/oobLoadedStatus.properties` file and update the **importSpaces.txt** property:

`importSpaces.txt=true`

6. Resynchronize the custom profile:
   a. Open the administrative console and click **System administration** > **Nodes**.
   b. Click **Full Resynchronize**.
7. Restart the cluster.

## Setting up security for Business Space

If you are using Business Space powered by WebSphere with your environment, you must consider security options for how your team will work with artifacts in Business Space. If you want to turn on security for Business Space, set up application security and designate a user repository. To define Business Space administrators, assign a superuser role.

For best results, enable security before you configure Business Space. If you enable security later, use the administrative console Global security administration page, to enable both administrative security and application security. On the same administrative console page, you also can designate a user account repository, including changing from the default federated repositories option to another user repository. To designate which users can perform Business Space administrator actions in the Business Space environment, assign the Business Space superuser role. Other security configuration may be needed for your specific environment.

**Important:** By default, the Ajax proxy configuration used with Business Space widgets does not restrict access to any IP addresses. For convenience, the Ajax proxy is configured by default to be open, which is not secure for production scenarios. To configure the Ajax proxy so that it displays only content from selected sites or blocks content from selected sites, follow the steps at Blocking IP addresses using the Business Space Ajax proxy.

**Enabling security for Business Space:**

If you expect to use a secured environment, enable security before you configure Business Space. However, if needed, you can enable security manually later. To turn on security for Business Space you must enable both application security and administrative security.

Before you complete this task, you must have completed the following tasks:

- Check that your user ID is registered in the user registry for your product.

Business Space is preconfigured to ensure authentication and authorization of access. Users are prompted to authenticate when accessing Business Space URLs. Unauthenticated users are redirected to a login page.

Business Space is configured to be accessed by HTTPS by default. If you prefer HTTP because your system is already behind a firewall, you can switch to HTTP by running the `configBSpaceTransport.py` script. The `configBSpaceTransport.py` script has parameters to switch to either HTTP or HTTPS if you want to change from a previous setting. See Designating HTTP or HTTPS settings for Business Space.

To enable authenticated access to Business Space, you must have a user registry configured and application security enabled. Authorization to spaces and page content in Business Space is handled internally to Business Space as part of managing spaces.

1. For complete instructions on security, see the security documentation for your product.
2. For the Business Space application, on the Global security administrative console page, select both **Enable administrative security** and **Enable application security**.
3. If you want to enable or remove security after you have configured Business Space with your profile, you must modify the **noSecurityAdminInternalUserOnly** property in the `ConfigServices.properties` file.

The **noSecurityAdminInternalUserOnly** property specifies the Business Space administrator ID when security is disabled. By default, Business Space configuration will set the property to **BPMAdministrator** if security is disabled. When security is enabled, by default this property is set to the application server admin ID. If you want to enable or remove security after you have configured Business Space, use the application server admin ID.

a. Modify the `ConfigServices.properties` file **noSecurityAdminInternalUserOnly** property to set it to the application server admin ID. The `ConfigServices.properties` file is located at *profile_root*`\BusinessSpace\`*node_name*`\`*server_name*`\mm.runtime.prof\config\ConfigService.properties` for a stand-alone server or *deployment_manager_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\config\ConfigService.properties` for a cluster.

b. Run the **updatePropertyConfig** command using the wsadmin scripting client.

   **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

   - For a stand-alone server:

     The following example uses Jython:

     ```
     AdminTask.updatePropertyConfig('[-serverName server_name -nodeName node_name
     -propertyFileName "profile_root\BusinessSpace\node_name\server_name
     \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
     AdminConfig.save()
     ```

     The following example uses Jacl:

     ```
     $AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name
      -propertyFileName "profile_root\BusinessSpace\node_name\server_name
     \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
     $AdminConfig save
     ```

   - For a cluster:

     The following example uses Jython:

     ```
     AdminTask.updatePropertyConfig('[-clusterName cluster_name -propertyFileName
      "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
     config\ConfigService.properties" -prefix "Mashups_"]')
     AdminConfig.save()
     ```

     The following example uses Jacl:

     ```
     $AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
      "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
     config\ConfigService.properties" -prefix "Mashups_"}
     $AdminConfig save
     ```

c. Restart the server.

d. Log into Business Space and reassign the owners of the default spaces to the new administrator ID.

- After the administrative security and application security are turned on, you receive a prompt for a user ID and password when you log on to Business Space. You must use a valid user ID and password from the selected user registry in order to log on. After you turn on administrative security, whenever you return to the administrative console, you must log on with the user ID that has administrative authority.
- If you want to change the user account repository from the default for your product profile, follow the steps in Selecting the user account repository for Business Space.
- If you have a cross-cell environment where Business Space is remote from where your product is running, and the nodes are not in the same cell, set up single-sign-on (SSO) and Secure Sockets Layer (SSL) certificates. Follow the instructions in Setting up SSO and SSL for Business Space.
- To designate who can perform Business Space administrator actions in the Business Space environment, see Assigning the Business Space superuser role.

**Selecting the user repository for Business Space:**

The federated repositories option is the default user account repository option for profiles. You can change the type of user account repository if needed for your environment.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

To enable authenticated access to Business Space, you must have a user registry configured and application security enabled. For information about application security, see "Enabling security for Business Space" on page 214.

Considerations for using a user account registry with Business Space:

- Based on the type of LDAP configuration that you are using, your settings can impact your ability to access Business Space correctly. Make sure that the user filters, the group filters, and mapping settings are configured properly. For more information, see Configuring Lightweight Directory Access Protocol search filters in the WebSphere Application Server documentation.
- Based on the type of federated repository configuration that you are using, your settings can affect your ability to access Business Space correctly. Make sure that the realms are configured properly. For more information, see Managing the realm in a federated repository configuration in the WebSphere Application Server documentation.
- The LDAP security is set up by default to use the login property `uid` (user ID) for searching in Business Space. If your LDAP security is changed to use another unique LDAP field, such as `mail` (email address) for the login property, then you must modify the **userIdKey** property in the `ConfigServices.properties` file in order for searching to work in Business Space. Follow step 3 below.
- If you are using a Microsoft SQL Server database and the **Standalone LDAP** registry, make sure that the user distinguished name (user DN) does not exceed 450 characters. If any of the user DN entries exceed 450 characters, you must designate the **Federated repositories** option for the user account repository.
- If you are using **Federated repositories**, you have additional capabilities in your widgets and framework, such as enhanced search capabilities. When searching for users to share spaces and pages, the search scope includes email, a full user name, and user ID.

1. On the Global security administrative console page, under **User account repository**, designate either **Federated repositories**, **Local Operating System**, **Standalone LDAP registry**, or **Standalone custom registry**.
2. Restart the server.
3. If you want to change the default user repository from the default **Federated repositories**, modify the **MashupAdminForOOBSpace** property in the `ConfigServices.properties` to designate the correct user ID (the UID property for your user repository) as the valid administrator ID.
   a. Copy the modified file into an empty folder on your system. The `ConfigServices.properties` file is located at *`profile_root`*`\BusinessSpace\`*`node_name`*`\`*`server_name`*`\mm.runtime.prof\config\ConfigService.properties` for a stand-alone server or *`deployment_manager_profile_root`*`\BusinessSpace\`*`cluster_name`*`\mm.runtime.prof\config\ConfigService.properties` for a cluster.
   b. Run the **`updatePropertyConfig`** command using the wsadmin scripting client.

      **Important:** For Windows, the value for the **`propertyFileName`** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

      - For a stand-alone server:

The following example uses Jython:

```
AdminTask.updatePropertyConfig('[-serverName server_name -nodeName node_name
-propertyFileName "profile_root\BusinessSpace\node_name\server_name
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

The following example uses Jacl:

```
$AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name
 -propertyFileName "profile_root\BusinessSpace\node_name\server_name
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- For a cluster:

  The following example uses Jython:

```
AdminTask.updatePropertyConfig('[-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

  The following example uses Jacl:

```
$AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

c. Log into Business Space and reassign the owners of the default spaces to the new administrator ID.

4. If you are using an LDAP repository with a unique LDAP field, such as `mail` (email address) for the login property instead of `uid` (user ID), modify the **userIdKey** property in the `ConfigServices.properties` file in order for searching to work in Business Space.
   a. Locate the `ConfigServices.properties` file at *profile_root*`\BusinessSpace\`*node_name*`\`*server_name*`\mm.runtime.prof\config\ConfigService.properties` for a stand-alone server or *deployment_manager_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\config\ConfigService.properties` for a cluster.
   b. Change the **userIdKey** attribute from `uid` to match the login property for your LDAP user repository, for example, `mail`.
   c. Copy the modified file into an empty folder on your system.
   d. Run the **updatePropertyConfig** command using the wsadmin scripting client.

      **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

      - For a stand-alone server:

        The following example uses Jython:

```
AdminTask.updatePropertyConfig('[-serverName server_name -nodeName node_name
-propertyFileName "profile_root\BusinessSpace\node_name\server_name
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

        The following example uses Jacl:

```
$AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name
 -propertyFileName "profile_root\BusinessSpace\node_name\server_name
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

      - For a cluster:

        The following example uses Jython:

```
AdminTask.updatePropertyConfig('[-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

The following example uses Jacl:

```
$AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

5. If you want to restrict logging in to Business Space to a subset of users and groups, you can change the mapping of the Business Space Java EE security role.
   a. Update the user/group mapping for two enterprise applications: **BSpaceEAR_*node_server*** and **mm.was_*node_server*** (for a stand-alone server environment) or **BSpaceEAR_*cluster*** and **mm.was_*cluster*** (for a network deployment environment).
   b. Click **Applications** > **Application Types** > **WebSphere enterprise applications** and select the two applications.
   c. In the right panel, under Detail Properties, select **Security role to user/group mapping**.
   d. Remap the **businessspaceusers** and **Allauthenticated** roles from the two applications by first removing the special subject.
   e. Click **Map Special Subjects** and select **None**.
   f. Click **Map Users** or **Map Groups** and assign each role to your selected users or groups.

   Changing the Java EE security role mapping does not affect the user/group search function in Business Space.
6. Restart the server.
7. Log in to Business Space and reassign the owners of the default spaces to the new administrator ID.

- To set authorization to pages and spaces in Business Space, you can manage authorization when creating Business Space pages and spaces.
- To designate who can perform Business Space administrator actions in the Business Space environment, see "Assigning the Business Space superuser role" on page 224.

**Note:**

If you find the following errors in the `SystemOut.log` file, you might have extra attributes in your user registry that cannot be processed:

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
    The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.ldap.LdapAdapter.setPropertyValue
(LdapAdapter.java:3338)
```

Set the following attributes in the `ConfigServices.properties` file to bypass those attributes:

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

The `ConfigServices.properties` file is located at *profile_root*`\BusinessSpace\`*node_name*`\`*server_name*`\mm.runtime.prof\config\ConfigService.properties` for a stand-alone server or *deployment_manager_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\config\ConfigService.properties` for a cluster. After modifying the `ConfigServices.properties` file, run the **updatePropertyConfig** command using the wsadmin scripting client by following the instructions in step 4.d.

**Note:**

If you have Java EE security enabled in a cluster, consider tightening the entry in the server policy applied to the Business Space help location.

The Business Space help location policy is:

**grant codeBase "file:${was.install.root}/profiles/***profile_name***/temp/***node_name***/-" {**

**permission java.security.AllPermission;**

**};**

Tighten the policy by changing it to:

**grant codeBase "file:${was.install.root}/profiles/***profile_name***/temp/***node_name***/***server_name***/BSpaceHelpEAR_***node_name_server_name***/BSpaceHelp.war/-" {**

**permission java.security.AllPermission;**

**};**

**Setting up SSO and SSL for Business Space:**

For remote environments where Business Space and your product server are in different cells, set up single-sign-on (SSO) and Secure Sockets Layer (SSL) configuration manually.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

**Tip:** If you have separate cells configured, make sure that SSO considerations are taken into account (including that LTPA keys are in synch, shared user names/realm names are in synch, and certificates are imported as appropriate). In some cases, with IBM Business Process Manager, there might be multiple repositories in the realm, which might result in a realm-mismatch error. See Managing the realm in a federated repository configuration in the WebSphere Application Server documentation.

1. If Business Space is remote from where your product is running, and if the node where Business Space is running and the node where your product is running are not in the same cell, you must complete manual steps to make sure that SSO is enabled. For example, if you are using more than one product, the servers are on different nodes, and you want them all to be able to work with the Business Space server, you must manually configure SSO. To enable SSO, complete the following steps:
   a. On the administrative console for each server, open the Global security page by clicking **Security** > **Global security**. Expand **Web and SIP security** and click **single sign-on (SSO)** to make sure that the **Enabled** check box is selected.
   b. Make sure that all the nodes use the same **User account repository** information (see step 3).
   c. Follow the steps in Import and export keys in the WebSphere Application Server information center.
2. If you are using HTTPS in the endpoints file, the endpoint location is on a different node than Business Space, and the SSL certificate is a self-signed SSL certificate, you must import it.

   Make sure that the signers are configured in the appropriate truststores for the Business Space server and the product server. See Secure communications using Secure Sockets Layer (SSL) in the WebSphere Application Server information center.

   For more information about SSO and SSL, see the WebSphere Application Server information center.

**Designating HTTP or HTTPS settings for Business Space:**

Business Space is configured to be accessed by HTTPS by default. If you want to change to HTTP, or you want to change back to HTTPS from a previous setting, use the `configBSpaceTransport.py` script.

The `configBSpaceTransport.jy` script is located in the *install_root*`\BusinessSpace\scripts` directory. Use the **allowhttp** value to change the `web.xml` to allow HTTP and HTTPS connections. Use the **httpsonly** value to change `web.xml` to allow only HTTPS and to redirect HTTP to HTTPS. Run the script on your stand-alone server or on the deployment manager for a clustered environment.

1. Locate the script *install_root*`\BusinessSpace\scripts\configBSpaceTransport.py` for designating HTTP or HTTPS settings.
2. Run the `configBSpaceTransport.py` with one the following options.
   a. To allow HTTP connections to Business Space, type the following command: `wsadmin -lang jython -user` *user_name* `-password` *password* `-f configBSpaceTransport.py -allowhttp` (allows both HTTP and HTTPS).
   b. To allow only HTTPS connections to Business Space, run: `wsadmin -lang jython -user` *user_name* `-password` *password* `-f configBSpaceTransport.py -httpsonly` (switches back to the default configuration, which always redirects HTTP to HTTPS).

   By default, the command applies to the current server name and node name, or on the current cluster, where you are running the command.

   If you want to designate a different location, use the optional **-serverName** and **-nodeName** parameters or the **-clusterName** parameter. For example, in a network deployment environment run the command from the deployment manager profile, but specify **-clusterName** for the cluster where Business Space is deployed to.

   **Note:** When the path contains a space, for example, if *install_root* is `My install dir`, you must enclose the path names in quotation marks.

**Setting up security for system REST services:**

To set up security for the data in the widgets based on users and groups, you must modify the users that are mapped to the REST services gateway application.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

How you map users to a REST service provider application affects all the services for the provider.

To see the affected services, select **Services** > **REST services** > **REST service providers**, and select the matching provider application in the list of providers.

1. On the administrative console, select one of the following options:
   - For a server environment, select **Applications** > **Application types** > **WebSphere enterprise applications** > **REST Services Gateway**
   - In addition, for a network deployment environment, select **Applications** > **Application types** > **WebSphere enterprise applications** > **REST Services Gateway Dmgr**
2. In the right panel, under Detail Properties, select **Security role to user/group mapping**.
3. To control access to the data in all the REST services widgets, add users and groups to the **RestServicesUser** role.

**Business Space widget security considerations:**

Depending on the widgets you use in Business Space with your business process management product, you might assign either administrative user group roles to control access to data in a widget, or you might assign an additional layer of role-based access for your widget.

**Administrative group roles and widgets**

You control access to data in widgets with administrative group roles and the users who are assigned to the administrative group roles. To see who is assigned to these roles, open the administrative console, select **Users and groups** > **Administrative group roles**, and select a group. The Roles list is displayed.

Business Rules and Business Variables are two examples of widgets that might require changes to the administrative group roles.

For the System Health widget, the following administrative roles all have monitoring permissions, allow access to the administrative console and, therefore, allow users assigned to those roles to access data in the System Health widget:

- **Monitor**
- **Configurator**
- **Operator**
- **Administrator**
- **Adminsecuritymanager**
- **Deployer**
- **iscadmins**

Users who are mapped to those administrative group roles have access to the data in the System Health widget. Users who are not mapped to those roles cannot access the data in the System Health widget.

**Configuring Tivoli Access Manager WebSEAL to work with Business Space:**

If you have Tivoli® Access Manager WebSEAL and you want to use it with Business Space, you must complete several additional configuration steps.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.
- Make sure that Tivoli Access Manager and IBM Business Monitor have the same users in the user registries.

**Topic scope:** This topic applies to the following products:

- IBM Business Monitor
- WebSphere Enterprise Service Bus
- IBM Business Process Manager

If you want to use Tivoli Access Manager WebSEAL with Business Space, you must configure WebSEAL to work with Tivoli Access Manager, configure WebSEAL to work with your product application server, and configure host junctions for your environment.

If you have IBM Business Process Manager and are configuring WebSEAL to work with Process Portal in your IBM BPM environment, follow the instructions at Configuring Tivoli Access Manager WebSEAL to work with Process Portal.

1. Configure WebSEAL to work with Tivoli Access Manager.
   a. Ensure that WebSEAL is installed and configured properly.
   b. To create a trusted user account in Tivoli Access Manager, which can be used for configuring TAI, issue the following commands:

      **pdadmin -a sec_master -p domino123**

      **pdadmin sec_master> user create -gsouser -no-password-policy taiuser "cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser**

      **pdadmin sec_master> user modify taiuser password-valid yes**

      **pdadmin sec_master> user modify taiuser account-valid yes**
   c. Create the junction between WebSEAL and your product application server using the **-c iv_creds** option for TAI++ and **-c iv_user** for TAI. Enter either of the following commands as one line, using the variables that are appropriate for your environment:

      For TAI++

      **server task webseald-server create -t tcp -b supply -c iv_creds**

      **-h *host_name* -p *websphere_app_port_number* /*junction_name***

      **Tip:** The *junction_name* must begin with **/**.
   d. In the WebSEAL configuration file *webseal_install_directory*/etc/webseald-default.conf, set the following parameter:

      **basicauth-dummy-passwd=*webseal_userid_passwd***

      For example, if you set the taiuser/ptaiuser in Tivoli Access Manager, set the following parameter:**basicauth-dummy-passwd = ptaiuser**

      If you are using a form-based authentication, set the following parameters:

      **forms-auth=both**

      **ba-auth=none**
2. If needed, configure WebSEAL to work with your product application server by enabling the TAI++ interceptor on the server.
   a. In the administrative console, select **Global security** > **Authentication mechanisms and expiration**.
   b. Expand **Web and SIP security**, and then select **Trust Association**. Select the check box and click **Apply**.
   c. To get **TAMTrustAssociationInterceptorPlus** to appear under **Interceptors**, add **com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus** and restart the server.
   d. Select **Interceptors** > **TAMTrustAssociationInterceptorPlus** > **custom properties**, and add the following properties:

| Name | Value |
|---|---|
| **com.ibm.websphere.security.webseal.configURL** | **${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties** |
| **com.ibm.websphere.security.webseal.id** | **iv-creds** |
| **com.ibm.websphere.security.webseal.loginId** | **taiuser** (if the user **taiuser/ptaiuser** was created in the Tivoli Access Manager) |

   e. Restart the cell.
   f. To access the client, go to https://*webseal_server_name*:*webseal_port*/*junction name*/*web_uri_for_client*.
3. Configure the host junctions for your environment, so that the Business Space widgets appear. Complete one of the following steps, depending on whether you are using virtual host junctions or transparent host junctions. Standard junctions are not supported.
   - If you are using virtual host junctions, create a virtual host junction. A virtual host junction eliminates the need to create separate junctions.

a. Make sure that a virtual host has been configured. Virtual host junctions match a host and port number and forward addresses to the target host. No URL filtering occurs, and all requests that match are forwarded to the target host.
b. Make sure that the following applications are available to the same virtual host. You may have some or all of the applications, based on which products you are using with Business Space.
   - BPMAdministrationWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus and IBM Business Process Manager)
   - BusinessSpaceHelpEAR_*nodename_servername* (for all products)
   - BSpaceEAR_*nodename_servername* (for all products)
   - BSpaceForms_*nodename_servername* (for all products)
   - HumanTaskManagementWidgets_*nodename_servername* (for IBM Business Process Manager and IBM Business Monitor)
   - PageBuilder2_*nodename_servername* (for all products)
   - REST Services Gateway (for all products)
   - REST Services Gateway Dmgr (for WebSphere Enterprise Service Bus and IBM Business Process Manager)
   - mm.was_*nodename_servername* (for all products)
   - WBMDashboardWeb_*nodename_servername* (for IBM Business Monitor)
   - wesbWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus)

   **Note:** This list of applications covers only the applications required by Business Space. You might need to add other applications to the list for non-Business Space scenarios using Tivoli Access Manager WebSEAL.
c. Run the following command using pdadmin: **server task** ***webseal server*** **virtualhost create -t** ***transport*** **-h** ***target_host*** **[-p** ***port***] **[-v** ***virtual_host_name***] ***virtual_host_label***

   Use the following information:
   - *webseal server* is the name of the WebSEAL server where you will create the virtual host entry.
   - *transport* is the type of transport. Valid entries are `tcp`, `ssl`, `tcpproxy`, and `sslproxy`.
   - *target_host* is the host of the required application.
   - *virtual_host_name* is used to match HTTP requests to a virtual host junction. If no value is entered, it is made up of the target host and port by default. For example, if you set the *virtual_host_name* to `myvirthost.ibm.com:80`, WebSEAL matches the URLs containing `myvirthost.ibm.com:80` and routes it to the host provided in the pdadmin command.
   - *virtual_host_label* is the label used to identify the entry in WebSEAL. It must be unique.

   For Business Space to run as expected, both `ssl` and `tcp` entries must be created for the type of transport. When you need both Secure Sockets Layer (SSL) and Transmission Control Protocol (TCP) to be supported in the same virtual host junction, you must use the `-g vhost_label` option, where *vhost_label* is the original virtual host label to share configuration. This option finds a previously created virtual host junction (one created earlier, where the *virtual_host_label* matches the label provided in the `-g` option), and shares that configuration. The second entry still requires its own *virtual_host_label*, but it can share the target host, port, and other values. If you do not provide this -g option, a second virtual host cannot be created because WebSEAL sees the target host and port as being identical to a previously created junction (which is not allowed).

- If you are using transparent host junctions, create a series of transparent path junctions for the widgets for each product.
  a. Review each context root you have defined. See Mapping Business Space URLs for a reverse proxy server).
  b. For each context root defined, run the following command using padmin: **server task** ***webseal server*** **create -t** ***transport type (ssl) or (tcp)*** **-x -h hostname** ***path***.

For example, type: **server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace**.

c. Update the following two properties in ConfigService.properties of the Business Space server:

```
reverseProxyHost = WebSEAL host
reverseProxyPort = WebSEAL port, for example: 80
```

d. Run the **updatePropertyConfig** command using the wsadmin scripting client.

- For a stand-alone server:

  The following example uses Jython:

  **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\ mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')**

  **AdminConfig.save()**

  The following example uses Jacl:

  **$AdminTask updatePropertyConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\ mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}**

  **$AdminConfig save**

- For a cluster:

  The following example uses Jython:

  **AdminTask.updatePropertyConfig('[-clusterName** *cluster_name* **-propertyFileName "***deployment_manager_profile_root***\BusinessSpace***cluster_name***\mm.runtime.prof\config\ ConfigService.properties" -prefix "Mashups_"]')**

  **AdminConfig.save()**

  The following example uses Jacl:

  **$AdminTask updatePropertyConfig {-clusterName** *cluster_name* **-propertyFileName "***deployment_manager_profile_root***\BusinessSpace***cluster_name***\mm.runtime.prof\config\ ConfigService.properties" -prefix "Mashups_"}**

  **$AdminConfig save**

4. Complete additional configuration steps to resolve issues with browser cookies and virtual hosts.

a. To resolve renaming of the Business Space cookie, add the following content to the WebSEAL configuration file:

```
[preserve-cookie-names]
name = com.ibm.bspace.UserName
name = com.ibm.wbimonitor.UserName
```

b. Optional: If you are using non-default virtual hosts with a context root, you might encounter issues with Business Space pages. You might need to stop the junction from rewriting the JavaScript on the Business Space pages by adding the -j junction to the context root. Run the following command: **server task default-webseald create -f -h** *hostname* **-p** *portnumber* **-t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/***context_root*

**Assigning the Business Space superuser role:**

In Business Space, you can assign users to be superusers (or Business Space administrators). A superuser can view, edit, and delete all spaces and pages, can manage and create templates, and can change ownership of a space by changing the owner ID.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

Assign the Business Space superuser role by using the following application server security role: **Admin**. Using this method gives you flexibility in assigning the role to any number of your organization's existing groups and users. It doesn't require the creation of an administrators group in the user registry for the sole purpose of acting as the focal point for the Business Space superuser.

If you already have the Business Space superuser assigned from an earlier version than V7.5, you can modify the superuser by user group instead. See Assigning the Business Space superuser by user group.

- If you are setting up the Business Space administrators with the superuser role for the first time, complete the following steps.
  1. Log in to the administrative console for your product.
  2. Click **Applications** > **Application Types** > **WebSphere enterprise applications** and select one of the following applications:
     - **mm.was_*node_server*** (for a stand-alone server environment)
     - **mm.was_*cluster*** (for a network deployment environment)
  3. Click **Security role to user/group mappings**.
  4. Select the row for the **Admin** role, and click the **Map Users** button or the **Map Groups** button to map either users or groups to the Admin role.
  5. Click **Save**.
  6. Restart the server.
- If you previously assigned superusers based on user groups, and you want to switch to this simpler way to manage superusers by role, complete the following steps.
  1. Open the configuration file.
     - For a stand-alone server: *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties
     - For a cluster: *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties
  2. Change the following property values in the configuration file.

     **com.ibm.mashups.adminGroupName = {com.ibm.mashups.J2EERole.Admin}**

     **com.ibm.mashups.widget.attributes.configure.groups=**
  3. Run the **updatePropertyConfig** command in the **wsadmin** environment of the profile.

     **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*\\BusinessSpace*node_name**server_name*\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.
     - For a stand-alone server:

       The following example uses Jython:

       ```
       AdminTask.updatePropertyConfig('[-serverName server_name -nodeName node_name
       -propertyFileName "profile_root\BusinessSpace\node_name\server_name
       \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
       AdminConfig.save()
       ```

       The following example uses Jacl:

       ```
       $AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name
        -propertyFileName "profile_root\BusinessSpace\node_name\server_name
       \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
       $AdminConfig save
       ```
     - For a cluster:

       The following example uses Jython:

```
AdminTask.updatePropertyConfig('[-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

The following example uses Jacl:

```
$AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
 "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

4. Restart the server.
5. Use the previous step to assign users to the Business Space superuser roles.

**Assigning the Business Space superuser by user group:**

You can assign Business Space users to be superusers (or Business Space administrators) based on user groups.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

**Tip:** If you previously used user groups to assign the Business Space superuser role, you can switch to the simpler way to assign Business Space superusers by role. See "Assigning the Business Space superuser role" on page 224.

A superuser can view, edit, and delete all spaces and pages, can manage and create templates, and can change ownership of a space by changing the owner ID.

If administrative security is enabled when you configure Business Space, consider the following information about groups and superusers:

- Users belonging to the special user group, **administrators**, have a superuser role by default. As a result, the superuser role assignment is handled by user group membership.
- In a single-server environment, the Business Space server creates the **administrators** user group in the default user registry. The administrator ID provided during configuration is automatically added as member of this group.
- In a network deployment environment, the **administrators** user group is not created automatically. Use the `createSuperUser.py` script to create the user group and add members to that group in the default user registry.
- If another user registry (for example, LDAP) is used instead of the default user registry, or if the default user registry is used but you do not want to use the **administrators** user group, you must identify the user group that you are using for the Business Space superusers. Make sure that the value you provide can be understood by the user registry. For example, for LDAP, you might provide a name like `cn=administrators,dc=company,dc=com`. For more information about identifying this user group, see the instructions for changing the administrators group in the What to do next section.
- For Business Space in WebSphere Portal, the default group **wpsadmins** is also used for the superuser role. Members of this group are granted the superuser role for Business Space.

  **Note:** Security must be enabled if you want to use Business Space in WebSphere Portal.

If administrative security is not enabled when you configure Business Space, only the special user ID **BPMAdministrator** has the Business Space superuser role.

If you have a network deployment environment, you must run the `createSuperUser.py` script to assign the superuser role: to create the user group and add members. Before you run the script, complete the following steps:

- Make sure the default **administrators** group name is not changed.
- Use the default repository for the user registry.
- Start the server or the deployment manager for your Business Space environment for the profile where is Business Space installed.

1. Locate the script *install_root*`\BusinessSpace\scripts\createSuperUser.py` for assigning the superuser role to a user.
2. Open a command prompt, and change directories to the following directory: *profile_root*`\bin`, where *profile_root* represents the directory for the profile where Business Space is installed.
3. Type the following command: `wsadmin -lang jython -f` *install_root*`\BusinessSpace\scripts\createSuperUser.py` *user_short_name password* where *user_short_name* is the unique identifier for a user in Virtual Member Manager (VMM), and *password* is the VMM password for that user. If that user exists in VMM, the user is added to the administrator group.

   **Note:** When the path contains a space, for example, if *install_root* is `My install dir`, you must enclose the path names in quotation marks. For example, type the following command: `wsadmin -lang jython -f "\My install dir\BusinessSpace\scripts\createSuperUser.py"` *user_short_name_in_VMM*.

To open Business Space, use the following URL: http://*host*:*port*/BusinessSpace, where *host* is the name of the host where your server is running and *port* is the port number for your server.

You can change the default special user group named **adminstrators**. Perform the following steps to check the current group name or change it to other name.

Inspect the value for the metric **com.ibm.mashups.adminGroupName** in the configuration file:

- *profile_root*`\BusinessSpace\`*node_name*`\`*server_name*`\mm.runtime.prof\config\ConfigService.properties` on a stand-alone server, or
- *deployment_manager_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\config\ConfigService.properties` on a cluster.

**Important:** For Windows, when you run the **updatePropertyConfig** command, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

If you want to change an administrative group, perform the following steps on a stand-alone server:

1. Make sure that the group exists in the user repository.
2. Modify the metric **com.ibm.mashups.adminGroupName** in the configuration file *profile_root*`\BusinessSpace\`*node_name*`\`*server_name*`\mm.runtime.prof\config\ConfigService.properties`.
3. Run the command updatePropertyConfig in the wsadmin environment of the profile:**$AdminTask updatePropertyConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}** and run **$AdminConfig save**.
4. Restart the server.

If you want to change an administrative group, perform the following steps on a cluster:

1. Make sure that the group exists in the user repository.

2. Modify the metric **com.ibm.mashups.adminGroupName** in the configuration file *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties.
3. Run the command updatePropertyConfig in the wsadmin environment of the deployment environment profile:**$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}** and run **$AdminConfig save**.
4. Restart the deployment manager.

If you want to change the superuser when security is not enabled, perform the following steps on a stand-alone server:

1. Modify the metric **noSecurityAdminInternalUserOnly** in the configuration file *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties.
2. Run the command updatePropertyConfig in the wsadmin environment of the profile:**$AdminTask updatePropertyConfig {-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}** and run **$AdminConfig save**.
3. Restart the server.

If you want to change the superuser when security is not enabled, perform the following steps on a cluster:

1. Modify the metric **noSecurityAdminInternalUserOnly** in the configuration file *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties.
2. Run the command updatePropertyConfig in the wsadmin environment of the deployment environment profile:**$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}** and run **$AdminConfig save**.
3. Restart the deployment manager.

**Preventing users from creating business spaces:**

You can customize Business Space so that only users logging in with a superuser role can create business spaces.

By default, all users can create business spaces. However, you can lock down Business Space so that only people who log in using a superuser ID can create or import business spaces.

**Important:** The lockdown procedure described in this topic applies only to the Business Space user interface. It does not restrict other access to Business Space.

These superusers (or Business Space administrators) can create a business space and transfer ownership to other users. The users who are assigned ownership of spaces can then administer the spaces as if they had created them. For example, they can set who can view and edit the space and its properties and they can add pages.

**Note:** The ability to prevent users from creating business spaces is not available for Business Space running on WebSphere Portal Server.

To limit creating business spaces to superusers only, complete the following steps.

1. Change the **com.ibm.mashups.lockeddown** setting to `true` in the configuration file:

- For a stand-alone server: *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties
- For a cluster: *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties

The default value of `false` means that all users can create business spaces. When the value is `true`, only superusers can create business spaces.

2. Run the **updatePropertyConfig** command in the **wsadmin** environment of the profile:
   - For a stand-alone server:

     The following example uses Jython:

     ```
     AdminTask.updatePropertyConfig('[-serverName server_name -nodeName node_name
     -propertyFileName "profile_root\BusinessSpace\node_name\server_name
     \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
     AdminConfig.save()
     ```

     **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*\\BusinessSpace*node_name**server_name*\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

     The following example uses Jacl:

     ```
     $AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name
      -propertyFileName "profile_root\BusinessSpace\node_name\server_name
     \mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
     $AdminConfig save
     ```

   - For a cluster:

     The following example uses Jython:

     ```
     AdminTask.updatePropertyConfig('[-clusterName cluster_name -propertyFileName
      "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
     config\ConfigService.properties" -prefix "Mashups_"]')
     AdminConfig.save()
     ```

     The following example uses Jacl:

     ```
     $AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName
      "deployment_manager_profile_root\BusinessSpace\cluster_name\mm.runtime.prof\
     config\ConfigService.properties" -prefix "Mashups_"}
     $AdminConfig save
     ```

The next time that users log into Business Space, they will not be able to create a business space unless they log in using a superuser ID.

**Enabling searches for user registries without wildcards:**

If your user registry is set up to not use wildcards, you must complete additional configuration steps so that searches work properly in Business Space and for widgets that search the user registry.

Before you complete this task, you must have completed the following tasks:

- Enable application security and administrative security. See "Enabling security for Business Space" on page 214.
- Check that your user ID is registered in the user registry for your product.

By default, when a Business Space user searches for users or groups by typing one or more characters, Business Space automatically adds wildcard characters. For example, if the user registry is an LDAP server and the user types `smit`, Business Space converts this into a `*smit*` query so that the return includes names like `Smith`, `Smithers`, and `Psmith`. However, if you do not want the automatic wildcards because, for example, your user registry does not permit them, you can disable this functionality.

To turn off the automatic wildcard searches for your environment, complete the following steps.

- For a stand-alone server, complete the following steps:
  1. Update the *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties configuration file with **com.ibm.mashups.user.stripWildcards=true**.
  2. Run the **updatePropertyConfig** command in the wsadmin environment of the profile:

     The following example uses Jython:

     **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')**

     **AdminConfig.save()**

     **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

     The following example uses Jacl:

     **$AdminTask updatePropertyConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}**

     **$AdminConfig save**
  3. Restart the server.
- For a cluster, complete the following steps:
  1. Update the *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties configuration file with **com.ibm.mashups.user.stripWildcards=true**.
  2. From the deployment manager, run the **updatePropertyConfig** command in the wsadmin environment of the profile:

     The following example uses Jython:

     **AdminTask.updatePropertyConfig('[-clusterName** *cluster_name* **-propertyFileName "***deployment_manager_profile_root***\BusinessSpace***cluster_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')**

     **AdminConfig.save()**

     The following example uses Jacl:

     **$AdminTask updatePropertyConfig {-clusterName** *cluster_name* **-propertyFileName "***deployment_manager_profile_root***\BusinessSpace***cluster_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}**

     **$AdminConfig save**
  3. Restart the deployment manager.

## Commands (wsadmin scripting) for configuring Business Space

Look up a scripting object or command class to find details about its command syntax.

The **wsadmin** tool is located under <*WAS_INSTALL_DIR*>/bin and <*WAS_PROFILE_DIR*>/bin. Use one of the following commands to launch it:

- For Jython:

  Windows **wsadmin -lang jython**

  Linux UNIX **./wsadmin.sh -lang jython**
- For Jacl:

Windows **wsadmin**

Linux UNIX **./wsadmin.sh**

For most of the Business Space commands, it is recommended that you run the **wsadmin** tool in disconnected mode (that is, with the server stopped). To do this, use the **-conntype NONE** parameter:

- For Jython:

  Windows **wsadmin -lang jython -conntype NONE**

  Linux UNIX **./wsadmin.sh -lang jython -conntype NONE**

- For Jacl:

  Windows **wsadmin -conntype NONE**

  Linux UNIX **./wsadmin.sh -conntype NONE**

To open the information center table of contents to the location of this reference information, click the **Show in Table of Contents** button on your information center border.

**addICMSystem command:**

Use the **addICMSystem** command to add the endpoints for IBM Case Manager services to the endpoint registry file for IBM BPM. This enables the federated REST API on the IBM BPM Advanced server to connect to the IBM Case Manager server.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

This command must be run where the IBM BPM federated REST API is deployed. If the application server is not running, include the `-conntype NONE` option when running this command.

**Required parameters**

**-icmCellName** *cell_name*
A parameter that specifies the name of the IBM Case Manager cell.

**-icmNodeName** *node_name*
A parameter that specifies the name of the IBM Case Manager node for the configuration. If you do not specify the **icmClusterName** parameter, you must specify both the **icmServerName** and **icmNodeName** parameters.

**-icmServerName** *server_name*
A parameter that specifies the name of the IBM Case Manager server for the configuration. If you do not specify the **icmClusterName** parameter, you must specify both the **icmServerName** and **icmNodeName** parameters.

**-icmClusterName** *cluster_name*
A parameter that specifies the name of the IBM Case Manager cluster for the configuration. For configuring Business Space on a cluster, you must specify the **icmClusterName** parameter without the **icmServerName** and **icmNodeName** parameters.

**-PEConnectionName** *connection_name*
A parameter that specifies the IBM Case Manager Process Engine connection name.

**-icmHostName** *host_name*
A parameter that specifies the name of the IBM Case Manager host.

**-icmPort** *port*
A parameter that specifies the port number of the IBM Case Manager host.

**-icmTransportType http | https**
A parameter that specifies whether the federated REST API uses the http or https protocol.

**Optional parameter**

**-federateSystem true | false**
If this is set to the value **true**, if the federation domain named **BPM_ICM_Federation_Domain** does not exist, it is created with two systems **ICM** and **BPM**. The default is false, which means no federation domain is created or modified. You can also manage the domain using the existing federation domain commands such as **modifyBPMApiFederationDomain**.

**Example**

The following examples uses the **addICMSystem** to add https endpoints for IBM Case Manager services on IBM BPM without adding the IBM Case Manager system to a federation domain.

Jython example:

```
AdminTask.addICMSystem('[-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name
 -icmHostName host_name
 -icmPort port
 -icmTransportType https
 -federateSystem false]')
```

Jacl example:

```
$AdminTask addICMSystem {-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name
 -icmHostName host_name
 -icmPort port
 -icmTransportType https
 -federateSystem false}
```

**configureBusinessSpace command:**

Use the **configureBusinessSpace** command to configure the database for Business Space powered by WebSphere.

This command configures the data source for Business Space and generates the scripts that create and configure database tables.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:
  `AdminConfig.save()`
- For Jacl:
  `$AdminConfig save`

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-nodeName** *node_name*
A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

**Optional parameters**

**-createTables true|false**
Specifies if you want to create the Business Space database tables. If the value is set to **true**, for DB2, Oracle, or SQL Server, the database is configured with Business Space tables. Setting this parameter to **true** requires that the Business Space database has been created before running this command. The default value is **false**.

**-dbName** *database_name*
Specifies the database that you are using for Business Space. If your application server and DB2 are on same z/OS image, you must specify the **-dbName** parameter.

**-dbWinAuth true|false**
Specifies if you are using Windows Authentication with Microsoft SQL Server. If you want to use Windows Authentication in your SQL Server environment, you must specify this parameter as**true**. The default is **false**.

**-schemaName** *schema_name*
An optional parameter that specifies the database schema for the Business Space database configuration. The default value is `IBMBUSSP`.

**-tablespaceDir** *table_space_path*
An optional parameter that specifies a directory path or file name prefix for the files used as the physical locations of table spaces. The default value is `BSP`. Valid for DB2, Oracle and SQL Server (otherwise ignored). For SQL Server, this parameter applies to the primary data file and log files.

**-tablespaceNamePrefix** *table_space_prefix*
An optional parameter that specifies a prefix string added to the beginning of table space names to make them unique. The default value is `BSP`. If a table space name prefix is longer than four characters, it is truncated to four characters. Valid for DB2, DB2 z/OS V8, DB2 z/OS V9, and Oracle (otherwise ignored).

**-dbLocationName** *database_location_name*
An optional parameter that specifies the database location name on z/OS. The default value is `BSP` or the product database name. Valid on DB2 z/OS V8 and V9 (otherwise ignored).

**-storageGroup** *storage_group*
An optional parameter that specifies the storage group on z/OS for Business Space. If you are using z/OS, you must update the database scripts that are generated before running them. For more information about the scripts, see Configuring Business Space database tables.

**-bspacedbDesign** *database_design_file_name*
An optional parameter that specifies a database design file that you are using to define all database configuration information, including the schema, and the table space directory. If you designate a database design file using the **-bspacedbDesign** parameter, you do not need to designate the **-schemaName**, **-tablespaceDir** , or **-storageGroup** parameters, unless you want to override what is in the database design file for particular database configuration information.

**Note:** The JNDI name of jdbc/mashupDS is always used for a Business Space data source, so the JNDI name in the database design file is not used. If a data source with a JNDI name of jdbc/mashupDS exists, this command stops without configuring the profile unless you also specify the **-replaceDatasource true** parameter.

**-productTypeForDatasource** *product_database*
An optional parameter that specifies properties to use to create the data source to use with Business Space. Designating a **productTypeForDatasource** creates a data source for Business Space with a JNDI name of jdbc/mashupDS that is modeled on the data source of an installed product, such as IBM Process Server, WebSphere Enterprise Service Bus, IBM Business Monitor, and WebSphere Business Compass. Valid values are `WPS` (to designate IBM Business Process Manager or WebSphere Enterprise Service Bus), `WPBS` (to designate WebSphere Business Compass), and `WBM` (to designate IBM Business Monitor). If the **bspacedbDesign** parameter is also specified, the **productTypeForDatasource** overrides the database type and JDBC provider, and the JNDI name in the database design file is not used.

**Note:** If a data source with a JNDI name of jdbc/mashupDS exists, this command stops without configuring the profile unless you also specify the **-replaceDatasource true** parameter.

**-replaceDatasource true|false**
An optional parameter that specifies whether the **configureBusinessSpace** command runs if the profile has already been configured. The default value is **false**. When a profile is configured for Business Space, a data source with a JNDI name of jdbc/mashupDS is created. If the data source exists and you run the **configureBusinessSpace** command without specifying **-replaceDatasource true**, the command does not change the configuration. If you specify **true**, the command deletes the data source and its JDBC provider, creates new ones, and creates new DDL scripts.

**–save true|false**
A parameter that indicates saving your configuration changes. The default value is **false**.

**Examples**

The following example uses the **configureBusinessSpace** command to configure a Business Space data source on a server.

- Jython example:

```
AdminTask.configureBusinessSpace('[-nodeName myNode -serverName
 myServer']')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-nodeName myNode -serverName
 myServer}
```

The following example uses the **configureBusinessSpace** to configure a Business Space data source on a cluster and save the changes.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster -save
 true]')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -save
 true}
```

The following example uses the **configureBusinessSpace** to configure a Business Space data source on a cluster, with a schema name and a product data source designated for IBM Process Server.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster
 -schemaName myCluster -productTypeForDatasource WPS -save true]')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-clusterName myCluster
 -schemaName myCluster -productTypeForDatasource WPS -save true}
```

The following example uses the **configureBusinessSpace** to configure a Business Space data source on a cluster using database information that is in the database design file.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster
 -bspacedbDesign "C:/BSpace_dbDesign.properties" -save true]')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-clusterName myCluster
 -bspacedbDesign "C:/BSpace_dbDesign.properties" -save true}
```

**createBPMApiFederationDomain command:**

Use the **createBPMApiFederationDomain** command to configure the federation domains in an environment with multiple deployment targets so that you can display processes and tasks created in Process Designer and Integration Designer in the same task list.

The **createBPMApiFederationDomain** command with the **addTarget** step creates a federation domain to federate tasks and processes across one or more deployment targets. The Federation API allows you to display processes and tasks created in Process Designer and Integration Designer in the same task list. The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands to create and manage federation domains. Use the **addTarget** step to add one or more deployment targets to a federation domain. The Federation API federates over all systems on the added deployment targets.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Target object**

Scope at which the federation domain is to be created. The target object can be used instead of the **nodeName**, **serverName** and **clusterName** parameters.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the name of the server on which the federation domain should be administered. If this parameter is specified, the **nodeName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is created on the cell scope.

**-nodeName** *node_name*
A parameter that specifies the name of the node on which the federation domain should be administered. If this parameter is specified, the **serverName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is created on the cell scope.

**-clusterName** *cluster_name*
A parameter that specifies the name of the cluster on which the federation domain should be administered. Do not specify this parameter if the **nodeName** and **serverName** parameters or a target object are specified. If no deployment target is specified, the federation domain is created on the cell scope.

**-name** *federation_domain_name*
The name of the new federation domain that you are creating. This name must be unique. This parameter is always required.

**Required parameters for the addTarget step**

**-targetCellName** *cell_name*
A parameter that specifies the name of the cell that is used as federation target. If this parameter is specified and the **nodeName**, **serverName** and **clusterName** parameters are not specified, the federation API federates across all systems in the cell.

**-targetNodeName** *node_name*
A parameter that specifies the name of the node that is used as federation target. If this parameter is specified, the federated API will federate across the systems on this node. If this parameter is specified, then the **targetServerName** parameter must be specified. Do not specify this parameter if the **targetClusterName** parameter is specified.

**-targetServerName** *server_name*
A parameter that specifies the name of the server that is used as federation target. If this parameter is specified, the federated API will federate across the systems on this server. If this parameter is specified, the **targetNodeName** parameter must be specified. Do not specify this parameter if the **targetClusterName** parameter is specified.

**-targetClusterName** *cluster_name*
A parameter that specifies the name of the cluster that is used as federation target. If this parameter is specified, the federated API federates across the systems on this cluster. Do not specify this parameter if the **targetNodeName** or **targetServerName** parameter are specified.

**Examples**

The following example uses the **createBPMApiFederationDomain** command to add a federation domain with the name **myCustomFederationDomain** that federates across a server (with the node name **myNode** and server name **myServer**) and a cluster (with the name **myCluster**).

- Jython example:

```
AdminTask.createBPMApiFederationDomain('[-nodeName node_name
 -serverName server_name -name myCustomFederationDomain
 -addTarget [["" myNode myServer ""] ["" "" "" myCluster]]]')
```

- Jacl example:

```
$AdminTask createBPMApiFederationDomain {-nodeName node_name
 -serverName server_name -name myCustomFederationDomain
 -addTarget {{"" myNode myServer ""} {"" "" "" myCluster}}}
```

**deleteBPMApiFederationDomain command:**

Use the **deleteBPMApiFederationDomain** command to delete a federation domain including the contained targets.

This command deletes a federation domain and its contained targets for federating tasks and processes across one or more deployment targets. The Federation API allows you to display processes and tasks created in Process Designer and Integration Designer in the same task list. The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands to create and manage federation domains.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Target object**

Scope at which the federation domain is to be deleted. The target object can be used instead of the **nodeName**, **serverName** and **clusterName** parameters.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the name of the server on which the federation domain should be administered. If this parameter is specified, the **nodeName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-nodeName** *node_name*
A parameter that specifies the name of the node on which the federation domain should be administered. If this parameter is specified, the **serverName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-clusterName** *cluster_name*
A parameter that specifies the name of the cluster on which the federation domain should be administered. Do not specify this parameter if the **nodeName** and **serverName** parameters or a target object are specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-name** *federation_domain_name*
The name of the federation domain that you want to delete. This name must be unique. This parameter is always required.

**Examples**

The following example uses the **deleteBPMApiFederationDomain** command to delete a federation domain

- Jython example:

```
AdminTask.deleteBPMApiFederationDomain('[-nodeName myNode -serverName myServer
-name myFederationDomain]')
```

- Jacl example:

```
$AdminTask deleteBPMApiFederationDomain {-nodeName myNode -serverName myServer
-name myFederationDomain}
```

**getBusinessSpaceDeployStatus command:**

Use the **getBusinessSpaceDeployStatus** command to check whether Business Space powered by WebSphere is configured on a particular deployment target.

This command checks whether Business Space is configured on a server, node, or cluster that you specify. If you don't set any parameters, it checks if Business Space is configured in the cell.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the server name to check for Business Space.

**-nodeName** *node_name*
A parameter that specifies the node name to check for Business Space.

**-clusterName** *cluster_name*
A parameter that specifies the cluster name to check for Business Space.

**Examples**

The following example uses the **getBusinessSpaceDeployStatus** command to check whether Business Space is configured on a server.

- Jython example:

```
AdminTask.getBusinessSpaceDeployStatus('[-nodeName myNode -serverName
 myServer]')
```

- Jacl example:

```
$AdminTask getBusinessSpaceDeployStatus {-nodeName myNode -serverName
myServer}
```

The following example uses the **getBusinessSpaceDeployStatus** command to check whether Business Space is configured on a cluster.

- Jython example:

```
AdminTask.getBusinessSpaceDeployStatus('[-clusterName myCluster]')
```

- Jacl example:

```
$AdminTask getBusinessSpaceDeployStatus {-clusterName myCluster}
```

The following example uses the **getBusinessSpaceDeployStatus** command to return a list of all deployment targets (server and clusters) configured for Business Space in a cell.

If you run the command from the profile root `bin` directory, the command returns a list of all deployment targets (server and clusters) configured for Business Space in a cell.

If you run the command from the installation root `bin` directory, the command returns a list of all deployment targets (server and clusters) configured for Business Space in the same installation root directory.

- Jython example:

```
AdminTask.getBusinessSpaceDeployStatus()
```

- Jacl example:

```
$AdminTask getBusinessSpaceDeployStatus
```

**installBusinessSpace command:**

Use the **installBusinessSpace** command to set up Business Space powered by WebSphere on your runtime environment.

The **installBusinessSpace** command can be used to install the Business Space enterprise archive (EAR) files in your runtime environment. It can also be used to update the configuration without installing Business Space.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:
  ```
  AdminConfig.save()
  ```
- For Jacl:
  ```
  $AdminConfig save
  ```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

Either serverName and nodeName, or clusterName are required.

**-serverName** *server_name*
A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both the **serverName** and the **nodeName** parameters.

**-nodeName** *node_name*
A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both the**serverName** and the **nodeName** parameters

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify the **clusterName** parameter.

**Optional parameters**

**–noWidgets true|false**
An optional parameter that if set to **true** prevents the product widgets from being installed on the deployment target. Then, if you want to install widgets, you must use the **installBusinessSpaceWidgets** command after the Business Space configuration has completed successfully. The default value is **false**.

**–save true|false**
An optional parameter that indicates saving your configuration changes. The default value is **false**.

**–configUpdateOnly true|false**
An optional parameter that if set to **true** only updates the configuration, without installing the Business Space enterprise archive (EAR) files on the deployment target. The default value is **false**.

**–configEnv** *environment*
An optional parameter that updates the profile settings to set the Business Space environment. The situations where you might need to use this parameter include:

- If you have augmented your IBM Business Process Manager Standard profile to include IBM Business Monitor, WebSphere Operational Decision Management, or IBM Case Manager, and you find that when you log onto Process Portal, you do not see the globe icon that allows users to switch to Business Space spaces that include widgets from these products. In this situation, you must run the **installBusinessSpace** command with **–configEnv bpm_adv** and **-configUpdateOnly true** to enable the globe icon. See “Examples: Enabling the globe icon in Process Portal” on page 240 later in this topic for an example.
- If, after creating a profile for a product that includes Business Space (such as WebSphere Business Monitor, IBM Case Manager, or WebSphere Operational Decision Management) in an environment

that includes an IBM Business Process Manager product, the Process Portal is available instead of Business Space. In this situation, manually switch back to the Business Space environment by completing the following steps:

1. Update the Business Space profile setting by running the **installBusinessSpace** wsadmin command with the **-configEnv business_space -configUpdateOnly true -save true** parameters.

   For example, if your Business Space is configured on a cluster named myCluster, use one of the following commands:

   – Using Jacl:

   ```
   $AdminTask installBusinessSpace {-clusterName myCluster -configUpdateOnly true -configEnv bspace2 -save true}
   ```

   – Using Jython

   ```
   AdminTask.installBusinessSpace(['-clusterName', 'myCluster', '-configUpdateOnly', 'true', '-configEnv', 'bspac
   ```

   If your Business Space is configured on a server, you must use the **-ServerName** and **-nodeName** parameters instead of the **-clusterName** parameter.

2. Edit the `install_root\profiles\`*`application_server_name`*`\BusinessSpace\`*`node_name`*`\`*`server_name`*`\mm.runtime.prof\public\oobLoadedStatus.properties` file and add the following three lines to it:

   ```
   importTemplates.txt=true
   importSpaces.txt=true
   importThemes.txt=true
   ```

3. Start or restart the server.
4. Clear the browser cache and then log into Business Space.

**Examples: Installing Business Space**

The following example uses the **installBusinessSpace** command to install Business Space EAR files on a server.

- Jython example:

  ```
  AdminTask.installBusinessSpace('[-nodeName myNode -serverName
   myServer -save true]')
  ```

- Jacl example:

  ```
  $AdminTask installBusinessSpace {-nodeName myNode -serverName
   myServer -save true}
  ```

The following example uses the **installBusinessSpace** to install Business Space EAR files on a cluster.

- Jython example:

  ```
  AdminTask.installBusinessSpace('[-clusterName myCluster -save true]')
  ```

- Jacl example:

  ```
  $AdminTask installBusinessSpace {-clusterName myCluster -save true}
  ```

**Examples: Enabling the globe icon in Process Portal**

The following cluster example uses the **installBusinessSpace** to enable the globe icon in Process Portal, that allows users to switch to Business Space spaces that include IBM Business Monitor widgets. This example does not install the Business Space EAR files. This example only applies if you have augmented your IBM Business Process Manager Standard profile to include IBM Business Monitor.

Jacl example:

```
wsadmin>$AdminTask installBusinessSpace {-clusterName myCluster -configUpdateOnly true
-configEnv bpm_adv -save true}
```

Jython example:

```
AdminTask.installBusinessSpace(['-clusterName', 'myCluster', '-configUpdateOnly', 'true',
'-configEnv', 'bpm_adv', '-save', 'true'])
```

**installBusinessSpaceWidgets command:**

Use the **installBusinessSpaceWidgets** command to install, deploy and register widgets for use with Business Space powered by WebSphere.

The **installBusinessSpaceWidgets** command installs, deploys, and registers designated widgets contained in a compressed file or an enterprise archive (EAR) file. If widgets are already deployed, the **installBusinessSpaceWidgets** command refreshes the binary and registration information.

The structure of the widget compressed file contains the following items:

- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:
  ```
  AdminConfig.save()
  ```
- For Jacl:
  ```
  $AdminConfig save
  ```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-nodeName** *node_name*
A parameter that specifies the node name for the configuration. Either a serverName, nodeName, or clusterName is required. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the configuration. For configuring Business Space widgets on a cluster, you must specify a **clusterName**.

**-widgets** *widgets_path*
A parameter that specifies one of the following:

- The full path for the directory that contains the compressed files or the EAR files that contain the widgets. If you specify a directory, all widgets will be installed for all compressed files and EAR files in that directory.
- The full path to an individual compressed file that contains the widgets.
- The full path to an individual EAR file that contains the widgets.

**–save true|false**
A parameter that indicates saving your configuration. The default value is **true**.

**Optional parameters**

**–save true|false**
A parameter that indicates saving your configuration. The default value is **true**.

**Examples**

The following example uses the **installBusinessSpaceWidgets** to install, deploy, and register widgets on a server.

- Jython example:

```
AdminTask.installBusinessSpaceWidgets('[-nodeName node_name
 -serverName server_name -widgets
 install_root/BusinessSpace/registryData/product_name/widgets/MyWidget.zip]')
```

- Jacl example:

```
$AdminTask installBusinessSpaceWidgets {-nodeName node_name
 -serverName server_name -widgets
 install_root/BusinessSpace/registryData/product_name/widgets/MyWidget.zip}
```

The following example uses the **installBusinessSpaceWidgets** to install, deploy, and register widgets on a cluster.

- Jython example:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName cluster_name
 -widgets X:/WPS/Temp]')
```

- Jacl example:

```
$AdminTask installBusinessSpaceWidgets {-clusterName cluster_name
 -widgets X:/WPS/Temp}
```

Manual steps are required for updating Business Space templates and spaces after running the **installBusinessSpaceWidgets** or **updateBusinessSpaceWidgets** command. For more information, see Updating Business Space templates and spaces after installing or updating widgets.

**installHumanTaskManagementWidgets command:**

Use the **installHumanTaskManagementWidgets** command to install the human task management widgets application on an IBM BPM Standard or IBM BPM Advanced server or cluster.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced with no Business Space configured

If you want to use the human task management widgets in a cross-cell configuration with IBM Case Manager you must use the **installHumanTaskManagementWidgets** command to install just the necessary widgets application.

**Required parameters**

**-clusterName** *cluster_name*
This parameter specifies the name of the IBM BPM cluster where the human task management widgets application will be installed. Normally, this should be the cluster where Business Space would be installed. For example, the application cluster in a one or two cluster topology, the support cluster in a three cluster topology, and the web application cluster in a four cluster topology.

If you specify the **clusterName** parameter, do not specify the **serverName** and **nodeName** parameters.

**-nodeName** *node_name*
This parameter specifies the name of the IBM BPM node where the human task management widgets application will be installed. If you do not specify the **clusterName** parameter, you must specify both the **serverName** and **nodeName** parameters.

**-serverName** *server_name*
This parameter specifies the name of the IBM BPM server where the human task management widgets application will be installed. If you configure Business Space later on the same server where the human task management widgets application is installed, the existing application will then be used by Business Space. If you do not specify the **clusterName** parameter, you must specify both the **serverName** and **nodeName** parameters.

**Example**

The following examples uses the **installHumanTaskManagementWidgets** to install the human task management widgets application on the **Support** cluster.

Jython example:

```
AdminTask.installHumanTaskManagementWidgets('-clusterClusterName Support')
AdminConfig.save()
```

Jacl example:

```
$AdminTask installHumanTaskManagementWidgets {-clusterClusterName Support}
$AdminConfig save
```

**listBPMApiFederationDomains command:**

Use the **listBPMApiFederationDomains** command to list all federation domains for your environment.

This command lists all federation domains that exist for a server or a cluster. The Federation API allows you to display processes and tasks created in Process Designer and Integration Designer in the same task list. The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands to create and manage federation domains.

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Target object**

Scope at which the federation domain is to be administered. The target object can be used instead of the **nodeName**, **serverName** and **clusterName** parameters.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the name of the server on which the federation domain should be administered. If this parameter is specified, the **nodeName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-nodeName** *node_name*
A parameter that specifies the name of the node on which the federation domain should be administered. If this parameter is specified, the **serverName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-clusterName** *cluster_name*
A parameter that specifies the name of the cluster on which the federation domain should be

administered. Do not specify this parameter if the **nodeName** and **serverName** parameters or a target object are specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**Examples**

The following example uses the **listBPMApiFederationDomains** command to list all federation domains on a server.

- Jython example:

```
AdminTask.listBPMApiFederationDomains('[-nodeName myNode -serverName
 myServer]')
```

- Jacl example:

```
$AdminTask listBPMApiFederationDomains {-nodeName myNode -serverName
myServer}
```

**modifyBPMApiFederationDomain command:**

Use the **modifyBPMApiFederationDomain** command to add or remove targets from a federation domain using the addTarget and deleteTarget steps.

This command adds or removes targets from a federation domain. The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands to create and manage federation domains. Use the **addTarget** step to add one or more deployment targets to a federation domain. Use the **deleteTarget** step to delete one or more deployment targets from a federation domain. The Federation API federates over all systems on the added deployment targets.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Target object**

Scope at which the federation domain is to be administered. The target object can be used instead of the **nodeName**, **serverName** and **clusterName** parameters.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the name of the server on which the federation domain should be administered. If this parameter is specified, the **nodeName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-nodeName** *node_name*
A parameter that specifies the name of the node on which the federation domain should be administered. If this parameter is specified, the **serverName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-clusterName** *cluster_name*
A parameter that specifies the name of the cluster on which the federation domain should be administered. Do not specify this parameter if the **nodeName** and **serverName** parameters or a target object are specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-name** *federation_domain_name*
The name of the new federation domain that you are modifying. This name must be unique. This parameter is always required.

**Required parameters for the addTarget and deleteTarget steps**

**-targetCellName** *cell_name*
A parameter that specifies the name of the cell that is used as federation target. If this parameter is specified and the nodeName, serverName and clusterName parameters are not specified, the federation API federates across all systems in the cell.

**-targetNodeName** *node_name*
A parameter that specifies the name of the node that is used as federation target. If this parameter is specified, the federated API will federate across the systems on this server. If this parameter is specified, then the targetServerName parameter must be specified. Do not specify this parameter if the targetClusterName parameter is specified.

**-targetServerName** *server_name*
A parameter that specifies the name of the server that is used as federation target. If this parameter is specified, the federated API will federate across the systems on this server. If this parameter is specified, then the targetNodeName parameter must be specified. Do not specify this parameter if the targetClusterName parameter is specified.

**-targetClusterName** *cluster_name*
A parameter that specifies the name of the server that is used as federation target. If this parameter is specified, the federated API federates across the systems on this cluster. Do not specify this parameter if the targetNodeName or targetServerName parameter are specified.

**Examples**

The following example uses the **modifyBPMApiFederationDomain** command to delete the deployment target **myNode**, **myServer** and add a new deployment target **myNewNode**, **myNewServer**.

- Jython example:

```
AdminTask.modifyBPMApiFederationDomain('[-nodeName node_name
-serverName server_name -name myCustomFederationDomain
-deleteTarget [["" myNode myServer ""]]')
-addTarget [["" myNewNode myNewServer ""]]]')
```

- Jacl example:

```
$AdminTask modifyBPMApiFederationDomain {-nodeName node_name
 -serverName server_name -name myCustomFederationDomain
 -deleteTarget {{"" myNode myServer ""}}
 -addTarget {{"" myNewNode myNewServer ""}}}
```

**registerRESTServiceEndpoint command:**

Use the **registerRESTServiceEndpoint** command to register configured and enabled Representational State Transfer (REST) endpoints so that your team can use the widgets in Business Space.

This command registers the REST service endpoints so that Business Space is properly connected to widgets for your product. This command registers the endpoints of the REST services that are in the same cell as Business Space.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

  ```
  AdminConfig.save()
  ```

- For Jacl:

  ```
  $AdminConfig save
  ```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-clusterName** *name_of_rest_services_cluster*
A parameter that specifies the cluster name for the REST service. When registering REST services endpoints for a cluster, you must specify a **clusterName**.

**-nodeName** *name_of_rest_services_node*
A parameter that specifies the node name for the REST service. When registering REST services endpoints for a server, you must specify both a **serverName** and a **nodeName**.

**-serverName** *name_of_rest_services_server*
A parameter that specifies the server name for the REST service. When registering REST services endpoints for a server, you must specify both a **serverName** and a **nodeName**.

**-businessSpaceClusterName** *name_of_business_space_cluster*
The Business Space cluster name. If Business Space is configured on a cluster, you must specify a **businessSpaceClusterName**.

**-businessSpaceNodeName** *name_of_business_space_node*
The Business Space node name. If Business Space is configured on a server, you must specify both a **businessSpaceServerName** and a **businessSpaceNodeName**.

**-businessSpaceServerName** *name_of_business_space_server*
The Business Space server name. If Business Space is configured on a server, you must specify both a **businessSpaceServerName** and a **businessSpaceNodeName**.

**Optional parameters**

**-appName** *name_of_provider_application*
The application name of the REST service provider.

**-name** *name_of_rest_service*
The name of the REST service.

**-type** *name_of_service_type*
The type of the service. This parameter is optional. If this parameter is not specified, all unique REST service endpoints configured for a specified REST service provider on a specified deployment target are registered. If you want to specify a specific service endpoint, use the **<tns:type>** value that is in the endpoints file for a widget. The service endpoints files are located at *install_root*\BusinessSpace\registryData*product_name*\endpoints directory. For example, bpmAdministrationEndpoints.xml contains all service endpoint types that are used by Administration widgets. The value of the **<tns:type>** element is **{com.ibm.bpm}SCA**:

```
<tns:Endpoint>
    <tns:id>{com.ibm.bpm}SCA</tns:id>
    <tns:type>{com.ibm.bpm}SCA</tns:type>
    <tns:version>6.2.0.0</tns:version>
    <tns:url>/rest/sca/v1</tns:url>
    <tns:description>Location backend SCA REST Services
 for Module Administration widgets and Service Monitoring widget
</tns:description>
  </tns:Endpoint>
```

For Jacl, make sure to use double quotation marks around the value, for example: **... -type "{com.ibm.bpm}SCA" ...**.

**-version** *name_of_version*
The version of the REST service provider.

**-webModuleName** *name_of_web_module*
The web module name of the REST service provider.

**Examples**

The following example uses the **registerRESTServiceEndpoint** command. It registers all configured and enabled REST services on the cluster with Business Space.

- Jython example:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster]')
```

- Jacl example:

```
$AdminTask registerRESTServiceEndpoint {-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster}
```

**removeICMSystem command:**

Use the **removeICMSystem** command to remove the endpoints for IBM Case Manager services from the endpoint registry file for IBM BPM.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

This command must be run where the IBM BPM federated REST API is deployed. If the application server is not running, supply the `-conntype NONE` option when running this command.

Although the **addICMSystem** command can be used to add an IBM Case Manager system to a federation domain, the **removeICMSystem** command cannot be used to remove a deployment target from a federation domain. That task must be performed using the federation domain administration commands.

**Required parameters**

**-icmCellName** *cell_name*
A parameter that specifies the name of the IBM Case Manager cell.

**-icmNodeName** *node_name*
A parameter that specifies the name of the IBM Case Manager node. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-icmServerName** *server_name*
A parameter that specifies the name of the IBM Case Manager server. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-icmClusterName** *cluster_name*
A parameter that specifies the name of the IBM Case Manager cluster. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-PEConnectionName** *connection_name*
A parameter that specifies the IBM Case Manager Process Engine connection name.

**Example**

The following example uses the **removeICMSystem** to remove the IBM Case Manager endpoints for IBM Case Manager services on a cluster.

Jython example:

```
AdminTask.removeICMSystem('[-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name')
```

Jacl example:

```
$AdminTask removeICMSystem {-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name}
```

**showBPMApiFederationDomain command:**

Use the **showBPMApiFederationDomain** command to display details about a federation domain.

This command displays details about the targets that are configured and the node, server, and cluster for a particular federation domain. The Federation API is automatically configured with your product as part of the REST Services Gateway application. If you want to change that configuration for your environment with multiple deployment targets, use wsadmin commands to create and manage federation domains.

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Target object**

Scope at which the federation domain is to be administered. The target object can be used instead of the **nodeName**, **serverName** and **clusterName** parameters.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the name of the server on which the federation domain should be administered. If this parameter is specified, the **nodeName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-nodeName** *node_name*
A parameter that specifies the name of the node on which the federation domain should be administered. If this parameter is specified, the **serverName** parameter must be specified. Do not specify this parameter if the **clusterName** parameter or a target object is specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-clusterName** *cluster_name*
A parameter that specifies the name of the cluster on which the federation domain should be administered. Do not specify this parameter if the **nodeName** and **serverName** parameters or a target object are specified. If no deployment target is specified, the federation domain is administered on the cell scope.

**-name** *federation_domain_name*
The name of the federation domain that you want to show. This name must be unique. This parameter is always required.

**Examples**

The following example uses the **showBPMApiFederationDomain** command to display details about a federation domain.

- Jython example:

```
AdminTask.showBPMApiFederationDomain('[-nodeName myNode -serverName
 myServer -name myFederationDomain]')
```

- Jacl example:

```
$AdminTask showBPMApiFederationDomain {-nodeName myNode -serverName
myServer -name myFederationDomain}
```

**uninstallBusinessSpaceWidgets command:**

Use the **uninstallBusinessSpaceWidgets** command to remove widgets and widget definitions from the profile, including removing individual widget assets (application, catalog, endpoints, spaces, templates, help).

The **uninstallBusinessSpaceWidgets** command removes widget files in a designated compressed file or an enterprise archive (EAR) file. The structure of the widget compressed file contains the following items:

- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

**Note:** If you customized REST endpoint information without using the **updateBusinessSpaceWidgets** command, those endpoint changes are lost after running the **uninstallBusinessSpaceWidgets** command.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-nodeName** *node_name*
A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

**-widgets** *widgets_path*
A parameter that specifies one of the following:

- the full path for the directory that contains the compressed files or the widget EAR files that contain the widgets. If you specify a directory, all widgets will be installed for all compressed files and EAR files in that directory.
- the full path to an individual compressed file that contains the widgets.
- the full path to an individual EAR file that contains the widgets.

**Optional parameters**

**–save true|false**
A parameter that indicates saving your configuration changes. The default value is **true**.

**Example**

The following example uses the **uninstallBusinessSpaceWidgets** command to remove widgets from a cluster.

**Note:** The examples are for illustrative purposes only. They include variable values and are not meant to be reused as snippets of code.

- Jython example:

```
AdminTask.uninstallBusinessSpaceWidgets('[-clusterName
 cluster_name -widgets X:/WPS/Temp]')
```

- Jacl example:

```
$AdminTask uninstallBusinessSpaceWidgets {-clusterName
cluster_name -widgets X:/WPS/Temp}
```

**updateBusinessSpaceWidgets command:**

Use the **updateBusinessSpaceWidgets** command to update previously configured Business Space widgets and their endpoints, catalogs, templates, and help plugins.

The **updateBusinessSpaceWidgets** command updates widget binary files, catalog files, endpoint files, templates, and help plug-ins for widgets that have been previously installed and configured for Business Space.

The **updateBusinessSpaceWidgets** command updates widget files in a designated compressed file or an enterprise archive (EAR) file. The structure of the widget compressed file contains the following items:

- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

```
AdminConfig.save()
```

- For Jacl:

```
$AdminConfig save
```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-serverName** *server_name*
A parameter that specifies the server name for the configuration. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

**-nodeName** *node_name*
A parameter that specifies the node name for the configuration. Either a serverName, nodeName, or clusterName is required. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

**Optional parameters**

**-widgets** *widget_path*
A parameter that specifies the full path for the directory where widget enterprise archive (EAR) files or widget compressed files are located or the full path to a specific EAR file or widget compressed file.

**-endpoints** *endpoint_path*
A parameter that specifies the full path for the directory where the widget endpoint files are located or the full path to a specific endpoint file.

**-catalogs** *catalog_path*
A parameter that specifies the full path for the directory that contains the widget catalog files or the full path to a specific catalog file.

**-templates** *template_path*
A parameter that specifies the full path for the directory that contains the widget template files or the full path to a specific template file.

**-helpplugins** *help_path*
A parameter that specifies the full path for the directory that contains the widget online help plugin files or the full path to a specific widget online help plugin file.

**–noWidgets true|false**
Specifies that you do not want to update the widget EAR files that are contained within the widgets compressed file.

**–noEndpoints true|false**
Specifies that you do not want to update the specified endpoint files that are contained in the widgets compressed file.

**–noCatalogs true|false**
Specifies that you do not want to update the catalog definition files that are contained in the widgets compressed file.

**–noTemplates true|false**
Specifies that you do not want to update the templates that are contained in the widgets compressed file.

**–noHelp true|false**
Specifies that you do not want to update the help files that are contained in the widgets compressed file.

**–save true|false**
A parameter that indicates saving your configuration. The default value is **true**.

**Examples**

The following example uses the **updateBusinessSpaceWidgets** to update widgets on a cluster.

Jython example:

```
AdminTask.updateBusinessSpaceWidgets('[-clusterName cluster_name
 -widgets widget_path]')
```

Jacl example:

```
$AdminTask updateBusinessSpaceWidgets {-clusterName cluster_name
 -widgets  widget_path}
```

The following example uses the **updateBusinessSpaceWidgets** to update widgets on a server.

Jython example:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName node_name
-serverName server_name -widgets widget_path]')
```

Jacl example:

```
$AdminTask updateBusinessSpaceWidgets {-nodeName node_name
 -serverName server_name -widgets  widget_path}
```

Manual steps are required for updating Business Space templates and spaces after running the **installBusinessSpaceWidgets** or **updateBusinessSpaceWidgets** command. For more information, see Updating Business Space templates and spaces after installing or updating widgets.

**updateRESTGatewayService command:**

Use the **updateRESTGatewayService** command to update a Representational State Transfer (REST) gateway service so that REST services are configured and enabled.

This command updates the REST Gateway service so that REST services are configured and enabled. The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page or the **updateRESTGatewayService** allows you to configure REST services for all of your product's widgets in Business Space.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:

  ```
  AdminConfig.save()
  ```

- For Jacl:

  ```
  $AdminConfig save
  ```

If the application server is not running, supply the `-conntype NONE` option when running this command.

**Required parameters**

**-clusterName** *cluster_name*
A parameter that specifies the cluster name for the REST service. For configuring REST services on a cluster, you must specify a **clusterName**.

**-nodeName** *node_name*
A parameter that specifies the node name for the REST service. For configuring REST services on a server, you must specify both a **serverName** and a **nodeName**.

**-serverName** *server_name*
A parameter that specifies the server name for the REST service. For configuring REST services on a server, you must specify both a **serverName** and a **nodeName**.

**-enable true | false**
Indicates if the REST service is enabled. Valid values include **true** or **false**.

**Optional parameters**

**-type** *name_of_service_type*
The type of the REST service.

**-version** *name_of_version*
The version of the REST service.

**Examples**

The following example uses the **updateRESTGatewayService** command to update the REST Gateway service so that REST services are configured and enabled.

- Jython example:

```
AdminTask.updateRESTGatewayService('[-nodeName node1 -serverName
 server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable
 true]')
```

- Jacl example:

```
$AdminTask updateRESTGatewayService {-nodeName node1 -serverName
 server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable true}
```

**Updating Business Space templates and spaces after installing or updating widgets:**

Manual steps are required for updating Business Space templates and spaces after running the **installBusinessSpaceWidgets** or **updateBusinessSpaceWidgets** commands in a clustered environment.

You must complete the following additional steps if you have previously used the **installBusinessSpaceWidgets** command or the **updateBusinessSpaceWidgets** command.

1. If Business Space is configured in a cluster, perform the following steps:
   a. Identify the custom profile for `oobLoadedStatus` `properties` file:
      1) In deployment manager profile, open the *deployment_manager_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\config\ConfigService.properties` file.
      2) Look for the name of cell, node and server in the **com.ibm.mashups.directory.templates** or `com.ibm.mashups.directory.spaces` properties.

         For example, in **com.ibm.mashups.directory.templates = config/cells/Cell01/nodes/Node01/servers/Server1/mm/templates**, you can locate the custom profile by the **Cell01** cell name and the **Node01** node name.
      3) Use the name of cell, node and server to locate the custom profile.
   b. In the custom profile, open the *custom_profile_root*`\BusinessSpace\`*cluster_name*`\mm.runtime.prof\public\oobLoadedStatus.properties` file and update the **importTemplates.txt** or **importSpaces.txt** properties:

      ```
      importTemplates.txt=true
      importSpaces.txt=true
      ```

      If you have created the Business Space database after it was deleted, or if you need to reload the theme for any other reason, also update the following property:

      ```
      importThemes.txt=true
      ```
   c. Resynchronize the custom profile.
      1) Open the administrative console and click **System administration** > **Nodes**.

2) Click **Full Resynchronize**.

d. Restart the cluster.

2. If Business Space is configured in a managed server, perform the following steps:

a. In the custom profile where the managed server is located, open the *custom_profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\public\oobLoadedStatus.properties file and update the **importTemplates.txt** or **importSpaces.txt** properties:

```
importTemplates.txt=true
importSpaces.txt=true
```

If you have created the Business Space database after it was deleted, or if you need to reload the theme for any other reason, also update the following property:

```
importThemes.txt=true
```

b. Resynchronize the custom profile.

1) Open the administrative console and click **System administration** > **Nodes**.

2) Click **Full Resynchronize**.

c. Restart the server.

## Configuring the Business Space Ajax proxy

You might want to modify the Business Space Ajax proxy for special considerations, such as changing timeout settings or blocking IP addresses for secure production environments.

The Ajax proxy file, proxy-config.xml, is located in the following locations:

- If you are using the Business Space environment that is shipped with your business process management product, *profile_root*/BusinessSpace/*node_name*/*server_name*/mm.runtime.prof/config/proxy-config.xml.

For issues with the Ajax proxy, see IBM Mashups tech notes at http://www-01.ibm.com/support/search.wss?tc=SSWP9P.

**Important:** The Ajax proxy is configured to be closed by default but provides a default policy that allows access to all Business Space endpoints. Follow the steps in Adding proxy polices to the Business Space Ajax proxy to allow access for additional URLs, and follow the steps in Blocking IP addresses using the Business Space Ajax proxy to restrict access to specific IP addresses.

1. Modify the proxy-config.xml file as needed.

   For example, if you are changing the timeout settings for the Business Space Ajax proxy, you modify the **proxy:value** for **socket-timeout**.

2. Run the **updateBlobConfig** command using the wsadmin scripting client, designating the **-serverName** and **-nodeName** parameters for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the proxy-config.xml file, and **-prefix** with the value **Mashups_**.

   The following example uses Jython:

   **AdminTask.updateBlobConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/config/proxy-config.xml" -prefix "Mashups_"]')**

   **AdminConfig.save()**

   The following example uses Jacl:

   **$AdminTask updateBlobConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "profile_root/BusinessSpace/node_name/server_name/mm.runtime.prof/config/proxy-config.xml" -prefix "Mashups_"}**

   **$AdminConfig save**

**Adding proxy policies to the Business Space Ajax proxy:**

Add additional proxy policies to the `proxy-config.xml` file so that Business Space works properly in a distributed environment.

The Business Space Ajax proxy contains predefined policies to some IBM URLs, but is not open to all URLs. If you use resources from remote sites in Business Space, add new policies in the `proxy-config.xml` file following the formatting of one of the predefined policies, such as the **<proxy:policy url="http://www-03.ibm.com/*" acf="none" basic-auth-support="true">**, to allow content from the remote sites to work properly in the Web Feed widget and the Google Gadgets widget.

If you had a previous version of Business Space, and you want the Ajax proxy to continue to be open to all URLs as it was in the previous version, change **<proxy:policy url="endpoint://*" acf="none" basic-auth-support="true">** to **<proxy:policy url="*" acf="none" basic-auth-support="true">**.

1. Open the `proxy-config.xml` file. For information about where to find the Ajax proxy file, see "Configuring the Business Space Ajax proxy" on page 254.
2. To restrict the Ajax proxy so that it allows access to only specific endpoints, make sure that the `proxy-config.xml` file contains **<proxy:policy url="endpoint://*" acf="none" basic-auth-support="true">** instead of **<proxy:policy url="*" acf="none" basic-auth-support="true">**.
3. Add policies for remote content.

   The following predefined policies allow access to web feeds from specific remote sites so that they work properly in the Web Feed widget.

   ```
   <proxy:policy url="http://www.ibm.com/*" acf="none" basic-auth-support="true">
   <proxy:actions>
   <proxy:method>GET</proxy:method>
   </proxy:actions>
   </proxy:policy>

   <proxy:policy url="http://www-03.ibm.com/*" acf="none" basic-auth-support="true">
   <proxy:actions>
   <proxy:method>GET</proxy:method>
   </proxy:actions>
   </proxy:policy>

   <proxy:policy url="http://www.redbooks.ibm.com/*" acf="none" basic-auth-support="true">
   <proxy:actions>
   <proxy:method>GET</proxy:method>
   </proxy:actions>
   </proxy:policy>
   ```

   To allow access to additional web feeds, Google Gadgets, or other remote content, add a policy like the following example:

   ```
   <proxy:policy url="http://your_URL" acf="none" basic-auth-support="true">
   <proxy:actions>
   <proxy:method>GET</proxy:method>
   </proxy:actions>
   </proxy:policy>
   ```
4. Complete the Ajax proxy configuration to fit your environment. See "Configuring the Business Space Ajax proxy" on page 254.

**Changing the timeout settings for the Business Space Ajax proxy:**

Business Space uses a proxy component to connect to your Representational State Transfer (REST) services. If REST services are not responsive, update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers.

If the REST service connections are timing out, update the following settings.

If you are using the Business Space environment that is shipped with your business process management product, the socket-timeout value is set to 30 seconds by default. Change it to an appropriate value for your situation.

If you are using Business Space with WebSphere Portal, the socket-timeout value is set to 10 seconds by default. Change it to an appropriate value for your situation (30 seconds, if you are using IBM Business Process Manager administration widgets).

1. Open the `proxy-config.xml` file. For information about where to find the Ajax proxy file, see "Configuring the Business Space Ajax proxy" on page 254.
2. Change the **proxy:value** for **socket-timeout**. The time is specified in milliseconds.

```
<proxy:meta-data>
 <proxy:name>socket-timeout</proxy:name>
 <proxy:value>30000</proxy:value>
</proxy:meta-data>
```

3. Complete the Ajax proxy configuration to suit your environment. For information, see "Configuring the Business Space Ajax proxy" on page 254.

**Blocking IP addresses using the Business Space Ajax proxy:**

The Ajax proxy forwards requests from widgets to your product and target servers, if the servers are remote from the Business Space server. The Ajax proxy is configured to be closed by default but provides a default policy that allows access to all Business Space endpoints. You can configure the Ajax proxy to restrict access to specific IP addresses.

**Important:** The Ajax proxy is configured to be closed by default but provides a default policy that allows access to all Business Space endpoints. Follow the steps in Adding proxy polices to the Business Space Ajax proxy to allow access for additional URLs, and follow the steps below to restrict access to specific IP addresses.

If you want to restrict access to specific IP addresses, you can edit the Ajax proxy to filter IP addresses to allow or deny access. You define blacklist or whitelist rules in the `proxy-config.xml` file.

1. Open the `proxy-config.xml` file. For information about where to find the Ajax proxy file, see "Configuring the Business Space Ajax proxy" on page 254.
2. Add filter rules that allow or deny access.

   To define a blacklist rule for a particular IP address or set of addresses, use a **proxy:deny** element. To define a whitelist rule for a particular IP address or set of addresses, use a **proxy:allow** element. The filter rules are applied in order, with the last applicable filter rule taking precedence over previous filter rules.

   Add the **<proxy:ipfilter>** information under the proxy rules of the `proxy-config.xml` file (after proxy policies and before **</proxy-rules>**).

```
<proxy:ipfilter>
<proxy:deny>9.6.0.0/255.255.0.0</proxy:deny>
<proxy:allow>9.6.1.0/255.255.255.0</proxy:allow>
<proxy:deny>9.6.1.4</proxy:deny>
</proxy:ipfilter>
```

   In this example, the IP filter performs the following filters:

   - blocks all 9.6.*.* IP addresses
   - allows 9.6.1.* but blocks the specific IP address 9.6.1.4

   So, in this case, the proxy would not allow access to IP address 9.6.2.5 or 9.6.120.7 and would respond with the following message: BMWPX0018E: The specified target hosts IP-address is prohibited by rule.

   The proxy would allow access to 9.6.1.5 or 9.6.1.120 but would deny access to 9.6.1.4.

   As you add new filter rules, you can combine them in several ways, but the proxy always handles them in order. The last matching rule will always take effect, regardless of any allow and deny rules that come before it.

3. Complete the Ajax proxy configuration to suit your environment. For information, see "Configuring the Business Space Ajax proxy" on page 254.

## Migrating Business Space (post-product migration)

After migrating your product to V8.0, you must perform some additional tasks for Business Space before you start your servers or clusters.

Before you start this task, you must have migrated your product server or cluster and verified that the migration was successful.

You also must have migrated the database that you use for Business Space. Follow the instructions specific to your product for migrating databases and data.

If you are migrating from an earlier version of your product and you have Business Space configured, you must complete the following steps after migration before you can use Business Space.

1. If you had custom widgets in a previous release, complete manual steps to make the widgets operational in Business Space V8.0. For more information, see Migrating custom widgets.

   **Tip:** The V7.0 data migration assists in migrating the widget catalog and endpoint of your custom widgets, so you do not need to manually migrate them again.
2. If you had an environment in the previous release with Business Space running on a different cell than the Representational State Transfer (REST) services, or with widgets on different cells than Business Space, you must update the endpoints files. For more information, see Enabling Business Space widgets for cross-cell environments.
3. If you used IBM Forms Server in your environment with Human Task Management widgets in a previous release, complete manual steps to get Business Space working with IBM Forms Server V4.0 and the Webform Server component.
   a. Install IBM Forms Server V4.0.
   b. In the administrative console for your product, update the following environment variables:
      - Change the **76** API references to **80**, for example: `${LFS_API_DIR};${LFS_API_DIR}/80/system;`
      - Change the value of the `LFS_DIR` variable to be the path of the IBM Forms Server installation, for example: `c:\Program Files\IBM Forms Server\4.0\WebformServer`.

      For more information, see Configuring IBM Forms Server for Human Task Management widgets in Business Space.
4. If you had exported spaces or templates from your previous Business Space environment, import them into Business Space V8.0 so that they are available to use. For more information, see Importing spaces and Importing templates.

   **Tip:** If you migrated from version 6.x, for templates, first import them as spaces in the Space Manager, then convert the imported spaces to templates by clicking **Actions** > **Save as Template**.

After you complete these migration procedures, you can use Business Space V8.0.

**Tip:** If you have used Business Space V6.2, you must clear your browser cache before using Business Space V8.0. This will help you avoid inadvertent, continued use of code and images from Business Space V6.2.

## Configuring Business Space to work with Mashup Center

If you configure Business Space to work with IBM Mashup Center, Business Space users can publish templates and pages to the Mashup Center catalog, use Mashup Center templates to create spaces, and import individual pages from Mashup Center into Business Space.

To use Business Space with Mashup Center, you must have a valid license for Mashup Center. Business Space only works with widgets registered in Business Space or widgets that have been published to the Mashup Center.

If Mashup Center (including IBM InfoSphere MashupHub) is not running on the same application server as Business Space, enable single-sign-on between the two application servers. To do this, your environment must be using a federated repository for your user registry. See Importing Lightweight Third Party Authentication keys and Exporting Lightweight Third Party Authentication keys in the WebSphere Application Server information center. Also, set up the SSL certificates. See Secure communications using Secure Sockets Layer (SSL) in the WebSphere Application Server information center.

To enable Business Space to work with Mashup Center, complete one of the following procedures for a stand-alone server or for a clustered environment.

- For a stand-alone server, complete the following steps:
  1. Modify the **com.ibm.mashups.hub.url** property in the *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ConfigService.properties configuration file and set it to the URL for the Mashup Center MashupHub component (***protocol*://*host*:*port*/mashuphub**).
  2. Run the **updatePropertyConfig** command in the wsadmin environment of the profile:

     The following example uses Jython:

     **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')**

     **AdminConfig.save()**

     **Important:** For Windows, the value for the **propertyFileName** parameter must be the full path to the file, and all backslashes must be double, for example: **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\\BusinessSpace***node_name******server_name***\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')**.

     The following example uses Jacl:

     **$AdminTask updatePropertyConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}**

     **$AdminConfig save**
  3. Open the *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\Endpoints.properties configuration file and change the **oob.Widget.url** property to the URL for Mashup Center (***protocol*://*host*:*port*/**).
  4. Run the **updatePropertyConfig** command in the wsadmin environment of the profile:

     The following example uses Jython:

     **AdminTask.updatePropertyConfig('[-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"]')**

     **AdminConfig.save()**

     The following example uses Jacl:

     **$AdminTask updatePropertyConfig {-serverName** *server_name* **-nodeName** *node_name* **-propertyFileName "***profile_root***\BusinessSpace***node_name******server_name***\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"}**

     **$AdminConfig save**
  5. Restart the server.
- On a cluster, complete the following steps:

1. Modify the **com.ibm.mashups.hub.url** property in the *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties configuration file and set it to the URL for the Mashup Center MashupHub component (***protocol://host:port/*mashuphub**).
2. From the deployment manager, run the **updatePropertyConfig** command in the wsadmin environment of the profile:

   The following example uses Jython:

   **AdminTask.updatePropertyConfig('[-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')**

   **AdminConfig.save()**

   The following example uses Jacl:

   **$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}**

   **$AdminConfig save**
3. Open the *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\Endpoints.properties configuration file and change the **oob.Widget.url** property to the URL for Mashup Center (***protocol://host:port/***).
4. From the deployment manager, run the **updatePropertyConfig** command in the wsadmin environment of the profile:

   The following example uses Jython:

   **AdminTask.updatePropertyConfig('[-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"]')**

   **AdminConfig.save()**

   The following example uses Jacl:

   **$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"}**

   **$AdminConfig save**
5. Restart the deployment manager.

## Configuring widgets to work with WebSphere Portal

If your team uses IBM WebSphere Portal, you can configure your Business Space widgets to work in the WebSphere Portal environment.

Before you configure widgets to work with WebSphere Portal, you must complete the following tasks:

- Install WebSphere Portal V7.0.0.2 Cumulative Fix 12 or later.
- Make sure that you have installed the WebSphere Portal V7.0.0.2 theme. See Theme enablement in the WebSphere Portal documentation.
- Make sure to apply the full profile to the pages that contain your widgets or to the entire theme. See the following topics in the WebSphere Portal documentation: Setting a profile override on a page and Changing the theme default profile.
- Install and configure your IBM product that includes Business Space V8.0.
- Configure Business Space, and configure Representational State Transfer (REST) services, so widgets can access the services during run time. For more information, see "Configuring REST services" on page 184.
- Configure SSL and SSO. For more information, see "Configuring SSO and SSL for widgets on WebSphere Portal" on page 263.

- Complete specific configuration steps for your widgets, if required.
- If you are using Human Task Management widgets in a clustered environment, make sure to install DOJO forms on the same node as the widgets.

When you set up Business Space widgets to work in WebSphere Portal, consider the following issues:

- Do not install your server product on a WebSphere Portal profile.

**Restriction:** Not all product widgets support running in WebSphere Portal. See your product's supported environments.

1. Create endpoint references on the WebSphere Portal application server. Business Space and product-specific endpoint reference entries must be created so that Business Space works properly in the WebSphere Portal environment. Endpoints must be defined on the WebSphere Portal server, but they are created remotely using the **updateEndpointBindingsOnPortal** command run on your product server.
   a. Start the WebSphere Portal server and your product server.
   b. Copy the service endpoint files from Business Space and your product to a temporary directory on your product machine, for example, `c:/tmp/endpoints/`.

      The service endpoint files are located on your product server in the following locations:

      - *profile_root*/BusinessSpace/*node_name*/*server_name*/mm.runtime.prof/endpoints/
      - *install_root*/BusinessSpace/registryData/*product_name*/endpoints

      Some endpoints files might exist in both locations. Copy only the service endpoint files for which you need to create entries. You don't need to copy a file that was previously processed using the **updateEndpointBindingsOnPortal** command. The following list includes IBM business process management examples of service endpoint files and widget endpoint files:

      - IBM Business Monitor: `monitorEndpoints.xml` and `monitorWidget.xml`
      - IBM Business Monitor with IBM Cognos Business Intelligence: `cognosEndpoints.xml` and `cognosWidget.xml`
      - WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `bpmAdministrationEndpoints.xml` and `BPMAdministrationWidgetEndpoints.xml` (for Administration widgets)
      - IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` and `BPMAdministrationWidgetEndpoints.xml` (for Administration widgets), `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `HumanTaskManagementEndpoints.xml` (for business processes and human tasks), `bspaceWFSEndpoints.xml` (for using Lotus Webform Server with Human Task Management widgets)
      - All products: `wsumEndpoint.xml` and `wsumWidget.xml` (for user membership)

   c. In a distributed environment, edit the service endpoint files to point to the correct URLs.

      Because endpoints are registered in the application server that hosts the WebSphere Portal server, it is required that all the endpoints point to the remote Business Space server. The endpoints must include the fully qualified name or IP of the remote host, for example:

      ```
      <tns:Endpoint>
          <tns:id>{com.ibm.bspace}bspaceCommonWidgetRootId</tns:id>
          <tns:type>{com.ibm.bspace}bspaceCommonWidgetRootId</tns:type>
          <tns:version>1.0.0.0</tns:version>
          <tns:url>http://<Business_Space_Host>:<port>/BusinessSpace/</tns:url>
          <tns:description>Location of Business Space Common Widgets</tns:description>
        </tns:Endpoint>
      ```

      Configure the endpoints as needed by editing the service endpoint files. Each endpoint in the file is designated by a **<tns:Endpoint>** block. Identify the block that you want to change. Look for comments that identify where you make the edits, for example:

```
<!-- When your REST service is remote from your Business Space server, update the following url
value with the fully qualified URL to the service.
For example https://host.domain.com:9443/rest/bpm/monitor/ -->
 <tns:url>/rest/bpm/monitor/</tns:url>
```

**Tip:** If you do not intend to activate some endpoints, you can remove them from the file to prevent confusion.

The location identified by an endpoint is specified in **<tns:url>**. This value is a path in a web module, specified as a full or relative HTTP URL. By default, the URL is relative. Change it to a full URL path, for example, **https://*virtualhost*.com:*virtualport*/rest/bpm/htm** or **http://host1:9445/WBPublishingDRAFT/**, where the protocol, host, and port identify how the product web module can be accessed.

To locate the port number for the server, perform the following steps:

- Log in to the administrative console.
- Click **Servers** > **Server Types** > **WebSphere application servers**.
- Click the server for which you want to find the port number, and then expand the Ports section.

All applications use the same port as shown in either the **wc_defaulthost** (unsecured host) parameter or the **wc_defaulthost_secure** (secure host) parameter.

**Important:** If you are using an HTTP server to access your web modules for load balancing, use the host name and port settings of the HTTP server.

d. Open a wsadmin session on your product server. Run wsadmin.bat or wsadmin.sh in the *profile_root*/bin/ directory. The wsadmin session connects to the local product application server Java virtual machine.

e. In the wsadmin session, run the **updateEndpointBindingsOnPortal** command. (In a network deployment environment, run it from the deployment manager.)

- Jython example:

  **AdminTask.updateEndpointBindingsOnPortal('[-nodeName** *Portal_node_name* **-serverName** *WebSphere_Portal* **-endpointBindingDirectoryName** *directory_containing_endpoints_files* **-host** *Portal_server_IP_or_host* **-port** *Portal SOAP_port_default_10025* **-user** *Portal_admin_ID* **-password** *Portal_admin_password*]')**

- Jacl example:

  **$AdminTask updateEndpointBindingsOnPortal {-nodeName** *Portal_node_name* **-serverName** *WebSphere_Portal* **-endpointBindingDirectoryName** *directory_containing_endpoints_files* **-host** *Portal_server_IP_or_host* **-port** *Portal SOAP_port_default_10025* **-user** *Portal_admin_ID* **-password** *Portal_admin_password*}

f. Restart the WebSphere Portal server.

g. From the WebSphere Portal administrative console, verify the endpoints by navigating to the resource environment provider named **WP Mashup Endpoints**. Click **Resources** > **Resource Environment** > **Resource Environment Providers** > **provider_name** > **Custom Properties**.

2. Configure the Ajax proxy on the WebSphere Portal server. To allow remote URLs to access your product server from the WebSphere Portal server, you must configure the Ajax proxy.

a. Update your existing proxy-config.xml file with the proxy policy example code snippet shown in "Required entries for the proxy-config.xml file to configure widgets to work with WebSphere Portal" on page 265.

b. Run the **checkin-wp-proxy-config** script.

In a clustered environment, run the script on the primary node.

**ConfigEngine.[bat|sh] checkin-wp-proxy-config -DProxyConfigFileName=***dir_path/temporary_proxy_file.name* **-DWasPassword=***application_server_password* **-DWasUserid=***application_server_user_ID* **-DPortalAdminId=***WebSphere_Portal_administrator_ID* **-DPortalAdminPwd=***WebSphere_Portal_administrator_password* where *dir_path/temporary_proxy_file.name* is the complete path of your modified wp.proxy.config.xml file.

For more information about the proxy configuration, see the WebSphere Portal documentation at http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global_proxy_configuration_wp7.

c. From the administrative console, restart the application named **AJAX Proxy Configuration**.

3. Register the Business Space widgets on WebSphere Portal.

   Business Space widgets are registered as iWidgets with WebSphere Portal by a bulk import using the WebSphere Portal-specific widget catalog file with your product. The catalog XML file is available at the root of the product web archive (WAR) file. Each product has a different context root.

   There are two types of widgets: common widgets and product-specific widgets.

   The context root for the common Business Space widgets is `/BusinessSpace`, and the catalog file is `catalog_commonWidgets_portal.xml`. For example, specify the URL to the catalog XML file for the common Business Space widgets as `http://localhost:9080/BusinessSpace/catalog_commonWidgets_portal.xml`.

   The following URLs are examples for business process management products:

   - IBM Business Monitor: http://*Business_Space_hosting_Monitor*:*port*/BusinessDashboard/catalog.xml
   - IBM Business Monitor with IBM Cognos Business Intelligence: http://*Business_Space_hosting_Monitor*:*port*/CognosWidgets/catalog.xml
   - Human Task Management widgets: http://*Business_Space_hosting_Business_Process_Manager*:*port*/HumanTaskManagementWidgets/portal_catalog.xml
   - Administration widgets:
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/BSpaceWidgetsHM/hmCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/PolymorphicWidget/polymorphicCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/scaWidget/scaCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/SecurityManagerWidgets/smCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/StoreAndForward/sfCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/ServiceMonitorGraphWidget/smGraphCatalog.xml
     - http://*Business_Space_hosting_Business_Process_Manager*:*port*/BSpaceWidgetsBCM/bcCatalog.xml

   a. Run the following command from *wp_profile*`\ConfigEngine` to register iWidgets using your product `catalog` XML file :

      **ConfigEngine.[bat|sh] register-iwidget-definition -DIWidgetCatalog=*URL_to_catalog_XML_file* -DWasPassword=*password* -DWasUserid=*ID* -DPortalAdminId=*ID* -DPortalAdminPwd=*password* -DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName**

      Example for IBM Business Monitor:

      **ConfigEngine.bat register-iwidget-definition -DIWidgetCatalog=http://localhost:9080/BusinessDashboard/catalog.xml -DWasPassword=admin -DWasUserid=admin -DPortalAdminId=admin -DPortalAdminPwd=admin -DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName**

   b. To verify that the command ran correctly, look for `Return Value:0`. For more information about optional commands, see the WebSphere Portal documentation at http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task_registeriwidgetdefinition_wp7.

After you have completed the setup for Business Space to work with WebSphere Portal, complete the following tasks:

- If you are using IBM Business Monitor with IBM Cognos Business Intelligence, you must update the `web.xml` file **ProxyServlet_Servlet** section. For more information, see the IBM Business Monitor documentation.

- To find and add specific Business Space iWidgets to a WebSphere Portal page and begin working in the WebSphere Portal environment, log in to the WebSphere Portal server and click **Actions** > **Edit Page**. The Business Space widgets are only visible under the **ALL** category. To find your widgets, select the **ALL** category and the name of the widget you want to add. Then, click the **Search** button.
- To enable the event exchange between iWidgets and native portlets on the same page in WebSphere Portal, and to enable the preservation of navigational states of widgets after switching pages, configure the pages that contain your Business Space widgets to use client side aggregation. For more information, see the WebSphere Portal documentation.
- When wiring your widgets, to ensure that all possible events of your widgets are shown, select **Consider semantic types or payload type for matching of sources and targets** as the matching mode. To change the matching mode, open the wiring editor and click **Settings**, then select **Consider semantic types or payload type for matching of sources and targets** and click **Done**.
- Make sure that the widgets shipped with your product are wired to work together. See the product documentation for your widget events. For example, for IBM Business Monitor, see Widget events.
- To see the titles of your widgets, you must set the theme to **Portal 7.0.0.2 - Standard**. The default in WebSphere Portal is that portlet titles are not displayed in View mode, which means that some of the widgets menus might not be displayed. To set the theme to **Portal 7.0.0.2 - Standard**, from the WebSphere Portal administrative console, click **Administration** > **Manage Pages**, for your page click **Edit page layout** > **AppearancePortal 7.0.0.2 - Standard**. Then you will see the portlet titles in View mode.

**Configuring SSO and SSL for widgets on WebSphere Portal:**

If you want your product widgets to work in WebSphere Portal, you must set up single sign-on (SSO) between WebSphere Portal and your product that includes Business Space widgets, and you must set up the Secure Sockets Layer (SSL) certificates so that they are exchanged between the WebSphere Portal and your product that includes Business Space widgets.

You must configure SSO between the servers for WebSphere Portal and your product that includes Business Space widgets. In addition, establish SSL between WebSphere Portal and your product that includes Business Space widgets. This requires that the SSL signer certificates are exchanged between the servers.

For the servers for both WebSphere Portal and your product, you must use the same user name and password to log on to the administrative console.

**Tip:** If you have separate cells configured, make sure that SSO considerations are taken into account (including that LTPA keys are in synch, shared user names/realm names are in synch, and certificates are imported as appropriate). In some cases, with IBM Business Process Manager, there might be multiple repositories in the realm, which might result in a realm-mismatch error. See Managing the realm in a federated repository configuration in the WebSphere Application Server documentation.

1. Set up SSO between WebSphere Portal and your product that includes Business Space widgets.
   a. Log on to the administrative console of the deployment manager for your product that includes Business Space widgets.
   b. Follow the steps in Import and export keys in the WebSphere Application Server information center.
2. Set up the SSL certificates so that they are exchanged between the servers of WebSphere Portal server and your product that includes Business Space widgets.

   Make sure that the signers are configured in the appropriate truststores for the WebSphere Portal server and your product server. See Secure communications using Secure Sockets Layer (SSL) in the WebSphere Application Server information center.

**updateEndpointBindingsOnPortal command:**

Use the **updateEndpointBindingsOnPortal** command to create endpoint references on the WebSphere Portal application server so that your team can use the widgets in Business Space on WebSphere Portal.

This command creates references to the Representational State Transfer (REST) endpoints on the WebSphere Portal application server. Business Space and product-specific endpoint reference entries must be created so that Business Space works properly in the WebSphere Portal environment. Business Space widgets are registered as iWidgets with WebSphere Portal by a bulk import using the WebSphere Portal-specific widget catalog file with your product. The catalog XML file is available at the root of the product web archive (WAR) file. Each product has a different context root. This command works only for the resource environment provider named **WP Mashup Endpoints**.

Before you run this command, you must install WebSphere Portal V7.0.0.1 or later, configure Business Space and REST services for your product, and configure SSL and SSO. For more information, see Configuring Business Space on WebSphere Portal.

After using the command, save your changes to the master configuration using one of the following commands:

- For Jython:
  ```
  AdminConfig.save()
  ```
- For Jacl:
  ```
  $AdminConfig save
  ```

**Required parameters**

**-serverName** *WebSphere_Portal_server_name*
A parameter that specifies the name of the target server for the WebSphere Portal configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-nodeName** *WebSphere_Portal_node_name*
A parameter that specifies the name of the target node for the WebSphere Portal configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

**-clusterName** *WebSphere_Portal_cluster_name*
A parameter that specifies the name of the target cluster for the WebSphere Portal configuration. For configuring Business Space on a cluster, you must specify only a **clusterName**. Do not specify a **serverName** or a **nodeName**.

**-host** *server_IP_or_host*
A parameter that specifies the IP or host name for the remote WebSphere Portal server. In a clustered environment, this parameter specifies the IP or host name of the Deployment Manager.

**-port** *SOAP_port*
A parameter that specifies the SOAP port name for the remote WebSphere Portal server; the default is 10025. In a clustered environment, this parameter specifies the SOAP port name of the Deployment Manager; the default is 8879.

**-user** *admin_ID*
A parameter that specifies the administrator ID for the remote WebSphere Portal server. In a clustered environment, this parameter specifies an ID with administrative rights on the Deployment Manager.

**-password** *admin_password*
A parameter that specifies the administrator password for the remote WebSphere Portal server or the Deployment Manager.

**-endpointBindingDirectoryName** *directory_containing_endpoints_files*
A parameter that specifies the directory that contains the endpoints files. Make sure that no other files exist in this directory.

**Examples**

The following example creates endpoint references on the WebSphere Portal application server for a stand-alone environment.

- Jython example:

  **AdminTask.updateEndpointBindingsOnPortal('[-nodeName** ***Portal_node_name*** **-serverName** ***WebSphere_Portal*** **-endpointBindingDirectoryName** ***directory_containing_endpoints_files*** **-host** ***Portal_server_IP_or_host*** **-port** ***Portal SOAP_port_default_10025*** **-user** ***Portal_admin_ID*** **-password** ***Portal_admin_password***]**')**

- Jacl example:

  **$AdminTask updateEndpointBindingsOnPortal {-nodeName** ***Portal_node_name*** **-serverName** ***WebSphere_Portal*** **-endpointBindingDirectoryName** ***directory_containing_endpoints_files*** **-host** ***Portal_server_IP_or_host*** **-port** ***Portal SOAP_port_default_10025*** **-user** ***Portal_admin_ID*** **-password** ***Portal_admin_password***}

The following example creates endpoint references on the WebSphere Portal application server for a clustered environment.

- Jython example:

  **AdminTask.updateEndpointBindingsOnPortal('[-nodeName** ***Portal_node_name*** **-serverName** ***WebSphere_Portal*** **-endpointBindingDirectoryName** ***directory_containing_endpoints_files*** **-host** ***DMGR_IP_or_host*** **-port** ***DMGR_SOAP_port_default_8879*** **-user** ***DMGR_admin_ID*** **-password** ***DMGR_admin_password***]**')**

- Jacl example:

  **$AdminTask updateEndpointBindingsOnPortal {-clusterName** ***Portal_cluster_name*** **-endpointBindingDirectoryName** ***directory_containing_endpoints_files_on_local_system*** **-host** ***DMGR_IP_or_host*** **-port** ***DMGR_SOAP_port_default_8879*** **-user** ***DMGR_admin_ID*** **-password** ***DMGR_admin_password***}

**Required entries for the proxy-config.xml file to configure widgets to work with WebSphere Portal:**

Use the examples of required entries for the `proxy-config.xml` file to configure the Ajax proxy on the WebSphere Portal server. To allow remote URLs to your product server from the WebSphere Portal server, you must configure the Ajax proxy.

The following XML snippet shows the proxy policy required for business process management products. This must be set for all remote URLs that you intend to open with the WebSphere Portal proxy, for example, the Business Space server and your business process management server. Replace **<REMOTE_BPM_URL>** with the remote URL that needs to be opened with the WebSphere Portal proxy.

**Tip:** The socket-timeout value is set to 10 seconds by default. Business Space uses a proxy component to connect to your Representational State Transfer (REST) services. If REST services are not responsive, change the socket-timeout value to an appropriate value for your situation, for example 30 seconds. See "Changing the timeout settings for the Business Space Ajax proxy" on page 255.

If you have multiple remote servers or URLs that need to be allowed with the proxy for the WebSphere Portal server, customize the proxy configuration by using dynamic policy entries. The proxy policy will differ from one deployment to the other. Refer to WebSphere Portal documentation for different ways to configure the WebSphere Portal server proxy.

The proxy-config.xml is located at *`WebSphere_Portal_install_root`*`\base\wp.proxy.config\installableApps\wp.proxy.config.ear\wp.proxy.config.war\WEB-INF`.

**Important:** The updated `proxy-config.xml` must be reviewed and approved by your WebSphere Portal administrators before being checked into WebSphere Portal.

```
<!-- BPM/Business Space proxy policy -->

<proxy:policy url="<REMOTE_BPM_URL>" acf="none">
<proxy:actions>
<proxy:method>GET</proxy:method>
<proxy:method>HEAD</proxy:method>
<proxy:method>POST</proxy:method>
<proxy:method>DELETE</proxy:method>
<proxy:method>PUT</proxy:method>

</proxy:actions>
<proxy:cookies>
<proxy:cookie>LtpaToken</proxy:cookie>
<proxy:cookie>LtpaToken2</proxy:cookie>
<proxy:cookie>JSESSIONID</proxy:cookie>
<proxy:cookie>CRN</proxy:cookie>
<proxy:cookie>caf</proxy:cookie>
<proxy:cookie>cam_passport</proxy:cookie>
<proxy:cookie>cc_session</proxy:cookie>
<proxy:cookie>userCapabilities</proxy:cookie>
<proxy:cookie>usersessionid</proxy:cookie>
</proxy:cookies>
<proxy:headers>
<proxy:header>User-Agent</proxy:header>
<proxy:header>Accept*</proxy:header>
<proxy:header>Content*</proxy:header>
<proxy:header>Authorization*</proxy:header>
<proxy:header>X-Method-Override</proxy:header>
<proxy:header>Set-Cookie</proxy:header>
<proxy:header>If-Modified-Since</proxy:header>
<proxy:header>If-None-Match</proxy:header>
<proxy:header>X-Server</proxy:header>
<proxy:header>X-Update-Nonce</proxy:header>
<proxy:header>X-Requested-With</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualhost</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualport</proxy:header>
<proxy:header>Slug</proxy:header>
<proxy:header>SOAPAction</proxy:header>
</proxy:headers>
</proxy:policy>

<proxy:meta-data>
<proxy:name>forward-http-errors</proxy:name>
<proxy:value>true</proxy:value>
</proxy:meta-data>
<proxy:meta-data>
<proxy:name>socket-timeout</proxy:name>
<proxy:value>30000</proxy:value>
</proxy:meta-data>
```

## Configuring Business Space to work with IBM Case Manager

If your team uses IBM Case Manager, you can configure IBM BPM human task management widgets to work in the IBM Case Manager environment. This allows users to work seamlessly with IBM BPM tasks and IBM Case Manager work items using an integrated inbox widget.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Before you configure human task management widgets to work with IBM Case Manager, you must complete the following tasks:

- Install and configure IBM Case Manager V5.1 or later, including Business Space, in one cell.

- Install and configure IBM Business Process Manager Standard or IBM Business Process Manager Advanced in another cell.

1. Configure cross-cell security, including SSO and SSL. Perform "Configuring cross-cell security for IBM BPM and IBM Case Manager."
2. Register the widgets in Business Space. Depending on where you have Business Space configured, perform one of the following.
   - If you are using Business Space on IBM Case Manager, perform "Registering IBM BPM widgets in IBM Case Manager" on page 270.
   - If you are using Business Space on IBM Business Process Manager Advanced, perform "Registering IBM Case Manager widgets in IBM Business Process Manager Advanced" on page 273.
3. Register the IBM Case Manager REST services in IBM BPM. Perform "Registering IBM Case Manager REST services in IBM BPM" on page 273.
4. Ensure that the necessary federation domain exists. If you did not use the **addICMSystem** command's **-federateSystem true** option to create the federation domain named **BPM_ICM_Federation_Domain** in the previous step, create a federation domain that contains the IBM BPM and IBM Case Manager cells. To do this, you can use the **createBPMApiFederationDomain** administration command. You can use a different domain name.

Now you can include an integrated inbox widget in a business space.

**Configuring cross-cell security for IBM BPM and IBM Case Manager:**

The products are configured in two different cells. Both cells need access the same users, single sign-on (SSO), and Secure Sockets Layer (SSL).

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Before you configure a cross-cell setup, complete the following tasks:

- Install and configure IBM Case Manager V5.1 or later in one cell.
- Install and configure IBM Business Process Manager Advanced or IBM Business Process Manager Standard in another cell.

1. Configure so that the IBM BPM and IBM Case Manager cells have access to the same users. There are different possible ways to achieve this, depending on your choice of user account repository. For example, if you have an existing LDAP server, you could make it available to both cells.
2. Identify the necessary search filters that match your user repository definitions. Both cells require identical filter strings for the following searches:
   - User
   - Group
   - Group membership

   You must inspect the definitions for your user repository to be able to determine the correct filter strings. For example, if you use a LDAP server that has the following definitions.
   - Group: **groupOfNames**
   - OrgContainer: **organization;organizationalUnit;domain;container**
   - PersonAccount: **inetOrgPerson**

   The appropriate search filters would be the following:
   - User search filter: **(&(objectClass=inetOrgPerson)(uid={0}))**
   - Group search filter: **(&(cn={0})(|(objectClass=groupOfNames)(objectClass=groupOfUniqueNames)))**

- Group membership search filter: **(|(&(objectclass=groupOfNames)(member={0}))( &(objectclass=groupOfUniqueNames)(uniqueMember={0})))**

3. Collect information about the user repository. Depending on the type of user repository you use, collect appropriate information such as the server host name, port number, login property, certificate mapping, and LDAP base entry distinguished name.
4. On the IBM Case Manager server, add the user directory to the federated realm.
   a. Start the Enterprise Manager and connect to the IBM Case Manager P8 domain.
   b. To start the Create a Directory Configuration wizard, right-click **Enterprise Manager**, select **Properties**, select the **Directory configuration** tab, and click **Add**. The Create a Directory Configuration Wizard window opens.
   c. Enter all the information that is required by the wizard about your user repository.
   d. Add a base entry for the user repositoryto the federated realm. In the administrative console, click **Security** > **Global Security** then in the **User account repository** section, click **Configure** > **Add base entry to realm** then enter the required information about the user repository. Click **OK** and **Save**.

      **Note:** If you use an LDAP server, make sure that you specify **EXACT_DN** for the certificate mapping.
   e. Restart the IBM Case Manager environment.
   f. Verify that you can search the user repository. In the administrative console, click **Users and Groups** > **Manage Users**. In the **Search for users** section enter a string in the **Search for** field that should match some existing users in the repository, for example **a***, click **Search** and verify that matching users are found.
5. On the IBM BPM server, add the user directory to the federated realm.
   a. Add a base entry for the user repositoryto the federated realm. In the administrative console, click **Security** > **Global Security** then in the **User account repository** section, click **Configure** > **Add base entry to realm** then enter the required information about the user repository. Click **OK** and **Save**.

      **Note:** If you use an LDAP server, make sure that you specify **EXACT_DN** for the certificate mapping.
   b. Restart the IBM BPM environment.
   c. Verify that you can search the user repository. In the administrative console, click **Users and Groups** > **Manage Users**. In the **Search for users** section enter a string in the **Search for** field that should match some existing users in the repository, for example **a***, click **Search** and verify that matching users are found.
6. Configure cross-cell single sign-on (SSO).
   a. Verify that automatic key generation is turned off. Perform the following steps for all participating cells for IBM BPM and IBM Case Manager.
      1) In the administrative console, click **Security** > **SSL certificate and key management** > **Manage endpoint security configurations**
      2) Expand the branches of the tree down to either the inbound or outbound management scope that contains the key set group, and then click the scope link for the cell.
      3) In the **Related Items** section, click **Key Set Groups**.
      4) Click the key set group **NodeLTPAKeySetGroup**.
      5) Clear the **Automatically generate keys** option.
      6) Click **OK** and **Save** to save the changes to the master configuration.
      7) Start the server again to activate the changes.
      8) Remember to perform steps 6a1 to 6a7 for all participating cells for both products.

b. Share a common LTPA key between all participating cells. As an example, the following steps illustrate exporting the LTPA key from the IBM BPM server and importing it into the keystore of one IBM Case Manager cell.
   1) In the IBM BPM administrative console click **Security** > **Global Security**, then in the **Authentication** section, click **LTPA**.
   2) In the **Cross-cell single sign-on** section enter a new strong password and a key file name. The file is created in the server's profile root directory unless a fully-qualified path is specified.
   3) Click **Export keys** then **OK**.
   4) Transfer the exported key file in binary mode to the file system of the IBM Case Manager cell.
   5) In the IBM Case Manager administrative console, click **Security** > **Global Security**, then in the **Authentication** section, click **LTPA**.
   6) In the **Cross-cell single sign-on** section enter the password and a key file name.
   7) Click **Import keys** then **OK**.
   8) If your setup includes more cells, repeat steps 6b4 to 6b7 for each additional cell.

c. Set the same domain name for SSO. Perform the following steps for all participating IBM BPM and IBM Case Manager. cells.
   1) In the administrative console, click **Security** > **Global Security**.
   2) In the **Authentication cache settings** section, expand **Web and SIP security**, then click **Single sign-on (SSO)**.
   3) In the **General Properties** section, specify the following configuration values:
      a) Select the **Enabled** option.
      b) For **Requires SSL**, enter the domain name that you are using for the servers, for example, **example.com**.
      c) Make sure that the **Interoperability Mode** and **Web inbound security attribute propagation** options are both selected.
      d) Click **OK** and save the changes to the master configuration.
   4) Remember to perform steps 6c1 to 6c3d for all participating cells.

d. Verify that SSO works across the cells. If you have Business Space configured on IBM BPM perform the following actions:
   1) Using a web browser, open the IBM BPM Business Space client by entering a URL similar to the following example **http://bpmserver.example.com:9080/BusinessSpace**.
   2) Log on using a user name and password that is stored in the shared LDAP server.
   3) Without closing the IBM BPM Business Space tab, press **Control-T** to open a new tab in the browser.
   4) In the new browser tab, open the IBM Case Manager case client by entering a URL similar to the following example **http://icmserver.example.com:9080/CaseClient**.
   5) If you are automatically logged in as the same user without having to enter a user ID and password in the case client then the SSO is working.

7. Configure SSL by exchanging the server SSL certificates.

a. Extract the root SSL certificate from the IBM BPM server. Perform the following actions using the administrative console on the IBM BPM server.
   1) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **DefaultTrustStore** > **Signer certificates**.
   2) Select the root certificate then click **Extract**.
   3) Enter a file name for the exported certificate, for example, `c:\bpmserverCert.pem`, and click **OK**.

   **Note:** If you are using a remote desktop connection, the exported certificate will be saved on the machine from which you started the administrative console.

b. Transfer the exported certificate file in binary mode to the IBM Case Manager file system.
c. Add the IBM BPM server certificate to the IBM Case Manager server. Perform the following actions using the administrative console on the IBM Case Manager server.
   1) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **DefaultTrustStore** > **Signer certificates**.
   2) Click **Add**.
   3) Enter an alias, for example, **bpmserver**.
   4) Enter the file name of the IBM BPM server certificate, for example, `c:\bpmserverCert.pem`, and click **OK**.
   5) Save the changes.
d. Extract the root SSL certificate from the IBM Case Manager server. Perform the following actions using the administrative console on the IBM Case Manager server.
   1) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **DefaultTrustStore** > **Signer certificates**.
   2) Select the root certificate then click **Extract**.
   3) Enter a file name for the exported certificate, for example, `c:\icmserverCert.pem`, and click **OK**.

   **Remember:** If you are using a remote desktop connection, the exported certificate will be saved on the machine from which you started the administrative console.
e. Transfer the exported certificate file in binary mode to the IBM BPM file system.
f. Add the IBM Case Manager server certificate to the IBM BPM server. Perform the following actions using the administrative console on the IBM BPM server.
   1) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **DefaultTrustStore** > **Signer certificates**.
   2) Click **Add**.
   3) Enter an alias, for example, **icmserver**.
   4) Enter the file name of the IBM BPM server certificate, for example, `c:\icmserverCert.pem`, and click **OK**.
   5) Save the changes.

The cross-cell setup is configured, including SSO and SSL.

Register the IBM BPM widgets in IBM Case Manager.

**Registering IBM BPM widgets in IBM Case Manager:**

Register the widget catalog and endpoints.

**Topic scope:** This topic applies to the following products:
- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

You have configured IBM Business Process Manager Advanced and IBM Case Manager in a cross-cell setup; including a federated realm. single-sign-on, and secure socket layer.

1. If you are using IBM BPM Standard, or an IBM BPM Advanced profile without Business Space, you must install the human task management widgets application on the IBM BPM server or cluster.
   a. Use the **`installHumanTaskManagementWidgets`** command to install the human task management widgets application on the IBM BPM server or cluster. For example, to install the human task management widgets application on the **Support** cluster, you can issue the following Jython commands:

```
AdminTask.installHumanTaskManagementWidgets('-clusterName Support')
AdminConfig.save()
```

b. Using the administrative console, locate the human task management widgets application named **HumanTaskManagementWidgets**_*scope*, and start it.

2. If you use BPEL tasks in IBM BPM Advanced, you must also deploy Dojo forms where the human task management widgets application is installed.
3. On the IBM BPM server, identify the host name and ports for the IBM BPM federated REST API. Because the widgets use both http and https protocols, note the port numbers for both protocols.
   - If you are using an HTTP server to access your web modules for load balancing or high availability, use the host name and port settings of the HTTP server.
   - For a stand-alone IBM BPM server, use the server host name. To identify the port numbers, in the administrative console, click **Servers** > **Server Types** > **WebSphere application servers** > *server_name*, and then expand the **Ports** section. The **wc_defaulthost** port is used for http connections and the **wc_defaulthost_secure** port is used for the https connections.
4. Copy the following files from the IBM BPM server to the IBM Case Manager server.
   - *install_root*\BusinessSpace\registryData\BPM\BPM_HumanTaskManagement_crosscell.zip
   - If you have IBM BPM Advanced also copy *install_root*\BusinessSpace\registryData\BPM\BPM_HumanTaskManagement_Advanced_crosscell.zip
5. Create a new directory.
6. Unpack all the ZIP files into the new directory. Verify that the following directories exist:
   - catalog
   - endpoints
   - templates
7. Define the endpoints for the REST services. Perform the following steps.
   a. Change to the endpoints directory. It should contain the following files.
      - HumanTaskManagementEndpoints.xml, which contains the endpoints for process and task services.
      - HumanTaskManagementWidgetsEndpoint.xml, which contains the endpoints for the human task management widgets and the predefined task forms. They must both be set to the host name and port number for the IBM BPM deployment target where Business Space is deployed or for which the **installHumanTaskManagementWidgets** command was run.
      - wsumEndpoint.xml, which contains the endpoint for the user membership services.
   b. Edit all the endpoint XML files in the endpoints directory. In each file, search for all **<tns:Endpoint>** tags, and change the value for **<tns:url>** to the fully qualified host name and port number for the IBM BPM REST API.

      For example, if your server's host name is **bpmserver.example.com** and it uses port 9080, you must change the endpoint URLs for Business Flow Manager (BFM) and Human Task Manager (HTM) to the federated versions of the URLs.
      - For BFM: **http://bpmserver.example.com:9080/rest/bpm/federated/bfm**
      - For HTM: **http://bpmserver.example.com:9080/rest/bpm/federated/htm**

      **Tip:** You can lookup the URLs for the REST services using the administrative console by clicking **Services** > **REST Services** > **REST Services**.
8. If you are using IBM Business Process Manager Advanced and your own BPEL process applications use Dojo forms, then you must register an endpoint for each web module that contains the Dojo forms. For each web module perform the following steps.
   a. Make a uniquely named copy of *install_root*\BusinessSpace\registryData\BPM\endpoints\CustomFormsEndpoint.xml in the endpoints directory that was created in step 6.
   b. Edit the endpoint file that you just copied.

1) Update the **tns:id** and **tns:type** values with a unique name for your web module. For example {com.example}myForms.
2) Update the **tns:url** value with the identical protocol, host name and port number that you set for the human task management widgets endpoint in step 7 on page 271. Use the context root of the web module that contains your Dojo forms.

9. On the IBM Case Manager server, in a wsadmin session, import the widget catalog and endpoint definitions by running the following Jython commands:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName node_name -serverName server_name
   -catalogs directory_containing_catalog_file
   -endpoints directory_containing_endpoints_files
   -templates directory_containing_templates_files]')
AdminConfig.save()
```

   Where *node_name* and *server_name* are the names of the node and server for the IBM Case Manager server. For a cluster, use the **-clusterName** parameter instead of **-nodeName** and **-serverName**. For more information about the **updateBusinessSpaceWidgets** command refer to the related information link.

10. Restart the IBM Case Manager server.

The Business Space widgets are registered in IBM Case Manager.

Configure the IBM Case Manager services in IBM BPM.

*installHumanTaskManagementWidgets command:*

Use the **installHumanTaskManagementWidgets** command to install the human task management widgets application on an IBM BPM Standard or IBM BPM Advanced server or cluster.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced with no Business Space configured

If you want to use the human task management widgets in a cross-cell configuration with IBM Case Manager you must use the **installHumanTaskManagementWidgets** command to install just the necessary widgets application.

**Required parameters**

**-clusterName** *cluster_name*
This parameter specifies the name of the IBM BPM cluster where the human task management widgets application will be installed. Normally, this should be the cluster where Business Space would be installed. For example, the application cluster in a one or two cluster topology, the support cluster in a three cluster topology, and the web application cluster in a four cluster topology.

If you specify the **clusterName** parameter, do not specify the **serverName** and **nodeName** parameters.

**-nodeName** *node_name*
This parameter specifies the name of the IBM BPM node where the human task management widgets application will be installed. If you do not specify the **clusterName** parameter, you must specify both the **serverName** and **nodeName** parameters.

**-serverName** *server_name*
This parameter specifies the name of the IBM BPM server where the human task management widgets application will be installed. If you configure Business Space later on the same server where the human task management widgets application is installed, the existing application will then be used by Business Space. If you do not specify the **clusterName** parameter, you must specify both the **serverName** and **nodeName** parameters.

**Example**

The following examples uses the **installHumanTaskManagementWidgets** to install the human task management widgets application on the **Support** cluster.

Jython example:

```
AdminTask.installHumanTaskManagementWidgets('-clusterClusterName Support')
AdminConfig.save()
```

Jacl example:

```
$AdminTask installHumanTaskManagementWidgets {-clusterClusterName Support}
$AdminConfig save
```

**Registering IBM Case Manager widgets in IBM Business Process Manager Advanced:**

To use the integrated inbox widget in the Business Space configuration on IBM Business Process Manager Advanced you must register the IBM Case Manager widgets in IBM Business Process Manager Advanced.

**Topic scope:** This topic applies to IBM Business Process Manager Advanced.

You have configured IBM Business Process Manager Advanced and IBM Case Manager in a cross-cell setup; including a federated realm. single-sign-on, and secure socket layer. Business Space is configured in IBM Business Process Manager Advanced.

1. Copy the contents of the *CASE_MANAGEMENT_INSTALLATION_PATH*/CaseWidgets/BusinessSpace/ConnectorForIBM_BPM_WidgetRegistration/ directory from the IBM Case Manager server to the IBM BPM server. This directory includes the subdirectories `catalog` and `endpoints`.
2. Define the endpoints for the REST services. Perform the following steps.
   a. Change to the `endpoints` directory.
   b. Edit the `acmwidgetsEndPoints.xml` file, and update the URL to point to the IBM Case Manager widgets.
3. On the IBM BPM server, in a wsadmin session, import the widget catalog and endpoint definitions by running the following Jython commands:

   ```
   AdminTask.updateBusinessSpaceWidgets('[-nodeName node_name -serverName server_name
      -catalogs directory_containing_catalog_file
      -endpoints directory_containing_endpoints_files]')
   AdminConfig.save()
   ```

   Where *node_name* and *server_name* are the names of the node and server for the IBM Business Process Manager Advanced server. For a cluster, use the **-clusterName** parameter instead of **-nodeName** and **-serverName**.
4. Restart the IBM Business Process Manager Advanced server.

The connector for theIBM BPM widget is registered in IBM Business Process Manager Advanced. When you log in to Business Space, the connector for the IBM BPM widget will be available.

Configure the IBM Case Manager services in IBM BPM.

**Registering IBM Case Manager REST services in IBM BPM:**

Run the **addICMSystem** command where the IBM BPM federated REST API is deployed.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard

- IBM Business Process Manager Advanced

1. Identify the following values for your IBM Case Manager system.
   - Cell name
   - Node and server names or cluster name
   - Process Engine connection name
   - Host name
   - Port number
   - The transport protocol used (http or https)
2. Decide whether to add the IBM Case Manager system to the federation domain for IBM BPM and IBM Case Manager using the **addICMSystem** command's **-federateSystem true** option. Alternatively you can create a suitable federation domain later.
3. Run the **addICMSystem** command where the IBM BPM federated REST API is deployed. The following examples add https endpoints for IBM Case Manager services on an IBM Business Process Manager Advanced cluster, and create the federation domain **BPM_ICM_Federation_Domain** with two systems, **ICM** and **BPM**.

   Jython example:

   ```
   AdminTask.addICMSystem('[-icmCellName cell_name
    -icmClusterName cluster_name
    -PEConnectionName connection_name
    -icmHostName host_name
    -icmPort port
    -icmTransportType https
    -federateSystem true]')
   ```

   Jacl example:

   ```
   $AdminTask addICMSystem {-icmCellName cell_name
    -icmClusterName cluster_name
    -PEConnectionName connection_name
    -icmHostName host_name
    -icmPort port
    -icmTransportType https
    -federateSystem true}
   ```

The IBM Case Manager REST services are registered in IBM BPM.

*addICMSystem command:*

Use the **addICMSystem** command to add the endpoints for IBM Case Manager services to the endpoint registry file for IBM BPM. This enables the federated REST API on the IBM BPM Advanced server to connect to the IBM Case Manager server.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

This command must be run where the IBM BPM federated REST API is deployed. If the application server is not running, include the `-conntype NONE` option when running this command.

**Required parameters**

**-icmCellName** *cell_name*
A parameter that specifies the name of the IBM Case Manager cell.

**-icmNodeName** *node_name*
A parameter that specifies the name of the IBM Case Manager node for the configuration. If you do not specify the **icmClusterName** parameter, you must specify both the **icmServerName** and **icmNodeName** parameters.

**-icmServerName** *server_name*
A parameter that specifies the name of the IBM Case Manager server for the configuration. If you do not specify the **icmClusterName** parameter, you must specify both the **icmServerName** and **icmNodeName** parameters.

**-icmClusterName** *cluster_name*
A parameter that specifies the name of the IBM Case Manager cluster for the configuration. For configuring Business Space on a cluster, you must specify the **icmClusterName** parameter without the **icmServerName** and **icmNodeName** parameters.

**-PEConnectionName** *connection_name*
A parameter that specifies the IBM Case Manager Process Engine connection name.

**-icmHostName** *host_name*
A parameter that specifies the name of the IBM Case Manager host.

**-icmPort** *port*
A parameter that specifies the port number of the IBM Case Manager host.

**-icmTransportType http | https**
A parameter that specifies whether the federated REST API uses the http or https protocol.

**Optional parameter**

**-federateSystem true | false**
If this is set to the value **true**, if the federation domain named **BPM_ICM_Federation_Domain** does not exist, it is created with two systems **ICM** and **BPM**. The default is false, which means no federation domain is created or modified. You can also manage the domain using the existing federation domain commands such as **modifyBPMApiFederationDomain**.

**Example**

The following examples uses the **addICMSystem** to add https endpoints for IBM Case Manager services on IBM BPM without adding the IBM Case Manager system to a federation domain.

Jython example:

```
AdminTask.addICMSystem('[-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name
 -icmHostName host_name
 -icmPort port
 -icmTransportType https
 -federateSystem false]')
```

Jacl example:

```
$AdminTask addICMSystem {-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name
 -icmHostName host_name
 -icmPort port
 -icmTransportType https
 -federateSystem false}
```

*removeICMSystem command:*

Use the **removeICMSystem** command to remove the endpoints for IBM Case Manager services from the endpoint registry file for IBM BPM.

**Topic scope:** This topic applies to the following products:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

This command must be run where the IBM BPM federated REST API is deployed. If the application server is not running, supply the `-conntype NONE` option when running this command.

Although the **addICMSystem** command can be used to add an IBM Case Manager system to a federation domain, the **removeICMSystem** command cannot be used to remove a deployment target from a federation domain. That task must be performed using the federation domain administration commands.

**Required parameters**

**-icmCellName** *cell_name*
A parameter that specifies the name of the IBM Case Manager cell.

**-icmNodeName** *node_name*
A parameter that specifies the name of the IBM Case Manager node. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-icmServerName** *server_name*
A parameter that specifies the name of the IBM Case Manager server. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-icmClusterName** *cluster_name*
A parameter that specifies the name of the IBM Case Manager cluster. Either specify both the **icmServerName** and **icmNodeName** parameters or the **icmClusterName** parameter.

**-PEConnectionName** *connection_name*
A parameter that specifies the IBM Case Manager Process Engine connection name.

**Example**

The following example uses the **removeICMSystem** to remove the IBM Case Manager endpoints for IBM Case Manager services on a cluster.

Jython example:

```
AdminTask.removeICMSystem('[-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name')
```

Jacl example:

```
$AdminTask removeICMSystem {-icmCellName cell_name
 -icmClusterName cluster_name
 -PEConnectionName connection_name}
```

## Configuring the global process monitor model

The global process monitor model enables you to monitor any BPEL process and Human Tasks without monitor model generation or deployment steps. Processes are detected dynamically and tracked based on the events they emit. The collected data can be viewed in Business Space using the Instances, KPIs, and reporting widgets.

For information about using the global process monitor model, see Global Process Monitor on the Business Process Management Samples and Tutorials website, or the developerWorks article provided in the Related information link.

## Installing the global process monitor model manually

If you chose not to install the global process monitor model when you created the IBM Business Monitor profile, you can install it later by following the steps below. The **GlobalProcessMonitorV75.ear** file is already stored on your hard disk drive even if you did not install the global process monitor model during profile creation. Use the administrative console to install this file.

To install the **GlobalProcessMonitorV75.ear** file, complete the following steps:

1. From the administrative console, click **Applications** > **Monitor Models**. This table lists all currently installed monitor models.
2. Click **Install**.
3. Select **Local file system** and click **Browse**.
4. Navigate to the folder that contains the .ear file: **app_server_root/installableApps.wbm/monitorModels**, select **GlobalProcessMonitorV75.ear**, and click **Open**.
5. Make sure that "Prompt me only when additional information is required" is selected.
6. Click **Next** and accept all defaults until you reach the Summary page.
7. On the Summary page, verify that all of the information is correct, and click **Finish**.
8. Optional. To review, click **Review changes** before saving or discarding.
9. Click **Save** to save to the master configuration and save the model.

If the processes you are planning to monitor will run on the same server, no further configuration is required. Otherwise the monitor model must be configured to receive events from the remote (IBM Business Process Manager) CEI as described in "Configuring how to receive events," as well as from the local (IBM Business Monitor server) CEI because the global process monitor model sends events to itself.

## Enabling events for the global process monitor model

To enable the global process monitor to track processes and human tasks, you must enable BPEL events generation using Integration Designer. The events you enable determine how much information IBM Business Monitor will have about the running processes and human tasks. Event generation for IBM Business Process Manager is enabled by default.

The following suggestions provide some general recommendations about the BPEL events to enable:

- For each process that you want to monitor, enable all events at the process level. Typically, there will be only a few events that a process issues during execution (start, end, failures, deletion).
- For each activity that is of interest to you (typically staff activities and invocations), also enable all events.
- For each staff activity that should be monitored, go to the Details tab of its Properties view and find the link to the corresponding human task (if it does not exist, click the Open button to create it). Follow the link to the human task, go to the Event Monitor tab of its Properties view, and then enable the required audit events.
- If you monitor both a process and a subprocess that it calls, enable all events for the invoke activity that links the two.
- Disable events for short-running, automated steps.
- Enable all events for stand-alone human tasks that you want to monitor.
- Consider enabling all events for loops, as that will give you a history of loop iterations with time stamps.
- Enable variable change events for the process variables that you want to monitor, and not for other process variables.

For more information on enabling event generation, refer to the Integration Designer 8.0 documentation. A link is provided below.

## Configuring your dashboards for the global process monitor model

The global process monitor receives events about processes and human tasks running in IBM Business Process Manager. It detects deployed process and task definitions based on the events that they emit as they run, and tracks the running processes and tasks. You can set up your own dashboard for this monitor model, using the Instances, KPIs, and reporting widgets, or you can use one of the provided business spaces as a starting point.

Two Business Space configurations are provided in the following locations:

- **app_server_root/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace.zip**
- **app_server_root/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace_Advanced.zip**

Both have the same overall structure, but the advanced version shows additional technical detail, such as millisecond precision and time zone information for time stamps; process and task instance identifiers, process instance migration histories, and audit event counts. Use the Import function in Business Space to upload the configuration that you prefer. You can use it as-is, or as a starting point to configure your personalized dashboard views.

For initial orientation, it might help to understand the monitoring context structure of this model:

```
Process Definition
    Process Execution
        Process Execution Step
            Related Task Execution
        Process Execution Variable
    Step Definition
        Step Execution
            Related Task Execution

Task Definition
    Task Execution
```

There are additional monitoring context definitions for data that could not be held in a metric and therefore required child monitoring contexts. These should be considered as data containers that are part of their parent monitoring context. They are not shown in the previous structure, which only highlights the main monitoring context structure of this monitor model.

A Process Definition monitoring context corresponds to a deployed process template in IBM Business Process Manager. It monitors that template and provides summary information for the number of times it was started, is still running, and has completed; the minimum, maximum, and average duration of runs; and so forth. Navigating down to a Process Execution monitoring context, you find information about a particular process run (start time, current state, completion time, and so forth). The children of a Process Execution context are the monitoring contexts for its individual steps (activities, human tasks, and so forth) and process variables.

Alternatively, you can navigate from a Process Definition monitoring context down to its Step Definition monitoring contexts to see all known steps of this process template. (Only steps that ran at least once and sent events to IBM Business Monitor can be detected.) Navigating down again, you arrive at the Step Execution level, where the same information is found as at the Process Execution Step level, except that it is grouped differently. Here you will find all executions of a given step definition instead of all steps that make up one process run.

When you configure dashboards, either your own custom dashboards or the supplied dashboards, you can choose which metrics to display in your widgets. Any metrics with **Aux** as a prefix in the metric name are for internal processing only, and you should not add these metrics to your dashboard.

# Chapter 11. Installing the showcase model

The single-server version of IBM Business Monitor comes with a mortgage lending sample model that illustrates some of the functionality of IBM Business Monitor. If you created a stand-alone profile, you can install the Better Lender showcase model using the First Steps console.

To install the Better Lender showcase model from the First Steps console, you must make sure that IBM Cognos Business Intelligence is installed and started.

If you created a stand-alone profile, you can use one of the following two methods.

- (Not for z/OS:) Install the showcase model using First Steps.
  1. Access First Steps from your stand-alone profile using one of the following options:
     - From the Profile Creation Complete panel, select the **Launch the IBM Business Monitor first steps** option.
     - Go to **Start** > **All Programs** > **IBM** > **Business Monitor 8.0** > **Profiles** > *profile_name* > **First Steps**.
     - Go to **profile_root\firststeps.wbm** and run the **firststeps.bat** command.

       **Important:** To install or run First Steps on Windows 7, Windows Vista, or Windows Server 2008, you must elevate your Microsoft Windows user account privileges by right-clicking **firststeps.bat** and selecting **Run as administrator**. This is required for both administrative and nonadministrative users.
     - Open a command window. Go to **profile_root/firststeps.wbm** and run the **firststeps.sh** command.
  2. From the First Steps console, select **Showcase model**.

     **Note:** If you have security enabled, you are prompted for the WebSphere Application Server user ID and password.
- Install the showcase model using the administrative console and then import the dashboards for the showcase model:
  1. To install the showcase model, click **Applications** > **Monitor models**. Click **Install** and navigate to the `MortgageLendingBAMApplication.ear` file, which is located in one of the following directories:
     - app_server_root/`installableApps.wbm/samples/mortgageLending/`
     - app_server_root\`installableApps.wbm\samples\mortgageLending\`

     Use the default settings for the installation.
  2. To import the dashboards for the showcase model, complete the following steps:
     a. Open a browser and enter the URL for Business Space that was provided by your administrator. For example, type `http://host_name:9080/BusinessSpace`.
     b. Enter your user name and password to log in.
     c. From the Welcome page, click **Manage Spaces**.
     d. Click **Import Space**.
     e. Click **Browse** and navigate to the showcase_dashboard.zip file, which is located in one of the following directories:
        - app_server_root/`installableApps.wbm/showcase/dashboards/7.5`
        - app_server_root\`installableApps.wbm\showcase\dashboards\7.5`

© Copyright IBM Corp. 2005, 2012

After the installation is complete, start the server and then open Business Space to view the Better Lender space. (The First Steps console provides options for both starting the server and launching Business Space.)

# Chapter 12. Updating IBM Business Monitor

You can install updates to IBM Business Monitor when they are available.

Visit the IBM Support website to check for available fix packs and interim fixes.

## Updating IBM Cognos BI

If you update IBM Cognos Business Intelligence or your Java Database Connectivity (JDBC) drivers, you must also regenerate the IBM Cognos BI enterprise archive (EAR) file. The deployed IBM Cognos BI service application must be updated with the new EAR file.

All nodes running the IBM Cognos BI service application must be running the same version and service level of IBM Cognos BI.

**Important:** Update only the base IBM Cognos BI directories (the directories under the WebSphere root). The copied runtime instances (directories under the profile) will be updated by IBM Business Monitor the next time that the IBM Cognos BI server starts.

To update IBM Cognos BI and the EAR file, complete the following steps:

1. To update IBM Cognos BI:
   a. Obtain the IBM Cognos BI service compressed file (tar.gz) for the platform type of your node.
   b. Unpack the file into a working directory.
   c. Locate and run the **issetup** command. When prompted for the installation location, enter app_server_root/cognos.

      **Tip:** UNIX Linux If you cannot run the graphical user interface of the update, or if you know that you do not have the MOTIF package installed, you must copy the silent installer from your existing IBM Cognos BI installation. Complete the following steps:

      1) Locate the following file in your existing IBM Cognos BI installation:

         ```
         app_server_root/cognos/uninstall/issetupnx
         ```

      2) Copy the file to the working directory of the new installer, placing it in the same directory as **issetup**.

      3) Update the file response.ats with the following values:

         ```
         I Agree=y
         APPDIR=app_server_root/cognos
         C8BISRVR_APP=1
         C8BISRVR_APPLICATION_TIER=1
         C8BISRVR_GATEWAY=1
         C8BISRVR_CONTENT_MANAGER=1
         C8BISRVR_CONTENT_DATABASE=1
         ```

      4) Open a command prompt in the working directory and run:

         ```
         ./issetupnx -s
         ```

2. To update the EAR file after updating IBM Cognos BI, complete the following steps:
   a. If you have updated your JDBC drivers, you must apply the new version to IBM Cognos Business Intelligence as well as to IBM Business Monitor. Before regenerating the EAR file, apply the new version to IBM Cognos BI in the following directories:

      ```
      app_server_root/cognos/webapps/p2pd/WEB-INF/lib
      app_server_root/cognos/v5dataserver/lib
      ```

   b. On your deployment manager or stand-alone server, open a command prompt in app_server_root/cognos/war/p2pd.

© Copyright IBM Corp. 2005, 2012

c. Run the following command:

**build.bat ear**

**build.sh ear**

This command creates a WebSphere EAR file called `p2pd.ear` in the IBM Cognos BI root directory. Building the EAR file might take several minutes.

d. On your deployment manager or stand-alone server, open the WebSphere administrative console and click **Applications** > **Application type** > **WebSphere enterprise applications**.

e. Select the **IBM Cognos** check box and click **Update**.

f. Under **Specify the path to the replacement ear file**, browse to the EAR file you created in Step c.

g. Complete the steps in the Update wizard to update the application. After you click **Finish**, the update might take several minutes.

h. Save your changes. Saving the new configuration might take several minutes.

i. Restart the application servers that were updated with the new IBM Cognos BI EAR file.

## Installing fix packs and interim fixes interactively

You can install updates to software packages using IBM Installation Manager interactively.

You cannot use this procedure to install updates on the underlying IBM DB2 Express or IBM Cognos BI. You must update these products following their normal update processes.

Visit the IBM Support website to check for available fix packs and interim fixes.

Before you install a fix pack or interim fix, perform the following tasks:

1. Read the fix pack and interim fix documentation thoroughly. The documentation lists dependencies, such as WebSphere Application Server fix pack levels or other IBM product fixes that you must install before you apply the fix pack or interim fix.
2. To ensure that your implementation is performing the same way that it did before you applied the fix pack or interim fix, prepare a regression test plan.
3. Back up your database and profile.
4. Before you deploy the fix pack or interim fix to a production environment, install the fix pack or interim fix in a development or quality-assurance environment.
5. You must perform the installation using the same user account that you used to install the product packages.

Each installed package has the location embedded for its default IBM update repository. For Installation Manager to search the IBM update repository locations for the installed packages, the preference **Search service repositories during installation and updates** on the Repositories preference page must be selected. This preference is selected by default.

During the update process, Installation Manager might prompt you for the location of the repository for the base version of the package. If you installed the product from DVDs or other media, they must be available when you use the update feature.

For more information about Installation Manager, see the information center link in related information.

**Important:** Any existing profiles are preserved and do not need to be recreated.

To find and install product package updates:

1. Stop all software for the product that you are updating. Close programs and stop servers that have profiles for this product.

2. Start Installation Manager. From the Start page of the Installation Manager, click **Update**.

   Windows You can also click **Start** > **Programs** > **IBM** > *package group name* > **Update**. For example, click **Start** > **Programs** > **IBM** > **IBM Business Monitor** > **Update**.
3. If IBM Installation Manager is not detected on your system or if an older version is already installed, then you must continue with the installation of the latest release. Follow the on-screen instructions in the wizard to complete the installation of IBM Installation Manager.
4. If you do not have Internet access, download the interim fix or fix pack locally, extract it to its own directory, and add the new directory to Installation Manager.
   a. Start Installation Manager.
   b. From the Start page, click **File** > **Preferences** > **Repositories**.
   c. From the Repositories page, click **Add Repository**.
   d. In the Add Repository window, browse to the directory where the extracted files for the interim fix or fix pack are located.
   e. Select the `repository.config` file and click **Open**.
   f. From the Repositories page, click **OK**.
5. In the Update Packages wizard, select the package group containing the product package you want to update or select the **Update all** check box, and then click **Next**. Installation Manager searches for updates in its repositories and the predefined update sites for the software you are updating. A progress indicator shows the search is taking place.
6. If updates for a package are found, then they are displayed in the **Updates** list on the Update Packages page below their corresponding package. Only the latest recommended updates are displayed by default. Click **Show all** to display all updates found for the available packages.
   a. To learn more about an update, click the update and review its description under **Details**.
   b. If additional information about the update is available, a **More info** link is included at the end of the description text. Click the link to display the information in a browser. Review this information before installing the update.
7. Select the updates that you want to install or click **Select Recommended** to restore the default selections, and click **Next**. Updates that have a dependency relationship are automatically selected and cleared together.
8. On the Licenses page, read the license agreements for the selected updates. On the left side of the Licenses page, the list of licenses for the updates you selected is displayed; click each item to display the license agreement text. If you agree to the terms of all the license agreements, click **I accept the terms of the license agreements**. Then click **Next**. If you do not accept the terms of the license agreements, you cannot install the fix pack or interim fix.
9. On the Summary page, review your choices before installing the updates.
   a. If you want to change the choices you made on previous pages, click **Back**, and make your changes.
   b. When you are satisfied, click **Update** to download and install the updates. A progress indicator shows the percentage of the installation completed.
10. Optional: When the update process completes, a message that confirms the success of the process is displayed near the top of the page. Click **View log file** to open the log file for the current session in a new window. You must close the Installation Log window to continue.
11. Click **Finish** to close the wizard.
12. Close Installation Manager.

## Installing fix packs silently

You can install fix packs to IBM Business Monitor silently.

Visit the IBM Support website to check for available fix packs and interim fixes.

Before you install a fix pack, perform the following tasks:

1. Read the fix pack documentation thoroughly. The documentation lists dependencies, such as WebSphere Application Server fix pack levels or other IBM product fixes that you must install before you apply the fix pack.
2. To ensure that your implementation is performing the same way that it did before you applied the fix pack, prepare a regression test plan.
3. Back up your database and profile.
4. Before you deploy the fix pack to a production environment, install the fix pack in a development or quality-assurance environment.
5. You must perform the installation using the same user account that you used to install the product packages.

You cannot use this procedure to install updates on the underlying IBM DB2 Express or IBM Cognos BI. You must update these products following their normal update processes.

To add a fix pack to IBM Business Monitor silently, complete the following steps:

1. Read the license terms before updating. Adding **-acceptLicense** to the command line means that you accept all license terms. If you do not accept the license, you cannot perform the installation.
2. Run the following command:

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.

   Windows

   ```
   extract_directory\IM\tools\imcl install list_of_product_IDs -acceptLicense -installationDirectory
   location -repositories repository -showVerboseProgress -log logName.log
   ```

   UNIX Linux

   ```
   extract_directory/IM/tools/imcl install list_of_product_IDs -acceptLicense -installationDirectory
   location -repositories repository -showVerboseProgress -log logName.log
   ```

   where:

   - *list_of_product_IDs* is a list of the IDs for the products you want to update, separated by spaces.

*Table 8. Product IDs*

| Product | Product ID |
|---|---|
| IBM Business Monitor | com.ibm.websphere.MON.V80 |
| IBM Business Monitor for z/OS | com.ibm.websphere.ZOS.MON.V80 |
| WebSphere Application Server Network Deployment | com.ibm.websphere.ND.v80 |
| WebSphere Application Base | com.ibm.websphere.BASE.v80 |

   - *extract_directory* is the path to where you extracted the fix pack files.
   - *location* is the path to the directory where you want to update the products.
   - *repository* is the path to the repository where you have extracted the fix pack files. For more than one repository, separate the repository locations with commas.
   - *logName* is the name of the log file to record messages and results.

Installation Manager updates the list of products and writes a log file to the directory that you specified.

The following example updates IBM Business Monitor on Windows.

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80 -acceptLicense
-installationDirectory C:\IBM\MON80 -repositories
D:\temp\MonServer\repository\fixpack1 -showVerboseProgress -log silentinstall.log
```

## Installing interim fixes silently

You can install an interim fix for IBM Business Monitor using the command-line mode of the Installation Manager.

Visit the IBM Support website to check for available fix packs and interim fixes.

Before you install an interim fix, perform the following tasks:

1. Read the interim fix documentation thoroughly. The documentation lists dependencies, such as WebSphere Application Server fix pack levels or other IBM product fixes that you must install before you apply the interim fix.
2. To ensure that your implementation is performing the same way that it did before you applied the interim fix, prepare a regression test plan.
3. Back up your database and profile.
4. Before you deploy the interim fix to a production environment, install the interim fix in a development or quality-assurance environment.
5. You must perform the installation using the same user account that you used to install the product packages.

This procedure uses a local directory to store the interim fix. For information about using an online repository that hosts the interim fix files and other configuration information, refer to the IBM Installation Manager information center.

To install an interim fix silently, complete the following steps:

1. Download the interim fix to the local system.
2. Create a new directory and extract the interim fix in the new directory.
3. Open a command prompt, and change directories to the `/eclipse/tools` directory under Installation Manager.

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.
4. Make the appropriate replacements and run the following command:

   ```
   imcl install fixID -repositories repositoryLocation -installationDirectory installationDirectory
   -log logLocation
   ```

   a. Replace ***fixID*** with the ID of the interim fix. The ID can be found in the `repository.xml` file in the directory where you extracted the interim fix, in the **fix id** element. For example:

   ```
   <fix id="8.0.0.0-WS-BPMADVWESB-IFJR39658" version="0.0.0.20111115_1047" offeringId="EnhancedFix"
   offeringVersion="0.0.0.EnhancedFix">
   ```

   b. Replace ***repositoryLocation*** with the directory where you extracted the interim fix.

   c. Replace ***installationDirectory*** with the location where you installed IBM Business Monitor.

   d. Replace ***logLocation*** with the location and file name to log the installation information.

   For example:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\tools>imcl install 8.0.0.0-WS-BPMADVWESB-IFJR39658
   -repositories C:\interimFix\8.0.0.0-WS-BPMADVWESB-IFJR39658/
   -installationDirectory C:\IBM\BPM80 -log logfix.txt
   ```

The installation log (specified by the **-log** parameter) contains no error messages if the interim fix installation is successful. The command line shows a message that the fix was installed. For example:

```
Installed 8.0.0.0-WS-BPMADVWESB-IFJR39658_0.0.0.20110525_1047 to the C:\IBM\BPM80 directory.
```

## Rolling back fix packs

Using the Roll back packages wizard, you can remove a fix pack from the IBM Business Monitor installation and revert to a previous version.

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your system when you install a package. If the files are not available on your workstation, you must include the location of the repository from which you installed the previous version of the product in your Installation Manager preferences (**File > Preferences > Repository**). If you installed the product from DVDs or other media, they must be available when you use the rollback function.

Use the rollback function if you have applied a fix pack to a product package, and decide later that you want to remove the update and revert to the earlier version of the product. When you use the rollback function, the Installation Manager uninstalls the updated resources, and reinstalls the resources from the previous version.

When you roll back to an earlier version of a package, it is restored with same features that were associated with that version. Use the Modify Packages wizard to add and remove features.

For more information about Installation Manager, including how to perform a rollback from the command line, refer to the Installation Manager information center.

1. Stop all software for the product that you are rolling back. Close programs and stop servers that have profiles for this product.
2. Start the Installation Manager.
3. From the Start page of the Installation Manager, click **Roll back** to start the Roll back packages wizard.
4. On the Roll Back Packages page, from the Package Group Name list, select the package group that contains the packages that you want to roll back and click **Next**.
5. Select the version of the package that you want to roll back to and click **Next**.
6. Read the summary information and click **Roll Back** to roll back the package.
7. Optional: When the rollback process completes, a message that confirms the success of the process is displayed near the top of the page. Click **View log file** to open the log file for the current session in a new window.
8. Click **Finish** to close the wizard.
9. Close Installation Manager.

The fix pack you selected to roll back is removed.

## Uninstalling interim fixes interactively

You can uninstall one or more interim fixes for IBM Business Monitor using Installation Manager.

You must perform the uninstallation using the same user account that you used to install the product packages.

**Important:** An interim fix cannot be uninstalled when another interim fix has a dependency on it, unless the dependent interim fix is also selected to be uninstalled. If you try to remove an interim fix that has a dependency on it from another interim fix, you will receive an error message.

To uninstall an interim fix interactively, complete the following steps:

1. Stop all software for the product that you are updating. Close programs and stop servers that have profiles for this product.
2. Start the Installation Manager. On the Start page, click **Uninstall**.
3. On the Uninstall Packages page, select the interim fix or fixes to uninstall and click **Next**.
4. Review your selection on the Summary page and then click **Uninstall**. After the uninstallation finishes, the Complete page opens.
5. Click **Finish** to exit the wizard.

The uninstallation of the interim fix or fixes is complete.

**Important:** Do not delete the Eclipse configuration directory after uninstalling the interim fix or fixes. Deleting this information will interfere with the operation of Installation Manager. By default, this is the `configuration` directory in the `install_root`.

## Uninstalling interim fixes silently

You can uninstall an interim fix for IBM Business Monitor using the command-line mode of the Installation Manager.

You must perform the uninstallation using the same user account that you used to install the product packages.

**Important:** An interim fix cannot be uninstalled when another interim fix has a dependency on it, unless the dependent interim fix is also selected to be uninstalled. If you try to remove an interim fix that has a dependency on it from another interim fix, you will receive an error message.

To uninstall an interim fix silently, complete the following steps:

1. Stop all software for the product that you are updating. Close programs and stop servers that have profiles for this product.
2. Open a command prompt, and change directories to the `/eclipse/tools` directory under Installation Manager.

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.
3. Make the appropriate replacements and run the following command:

   `imcl uninstall` ***fixID*** `-installationDirectory` ***installationDirectory*** `-log` ***logLocation***

   a. Replace ***fixID*** with the ID of the interim fix. The ID can be found in the `repository.xml` file in the directory where you extracted the interim fix, in the **fix id** element. For example:

   ```
   <fix id="8.0.0.0-WS-BPMADVWESB-IFJR39658" version="0.0.0.20111115_1047" offeringId="EnhancedFix"
   offeringVersion="0.0.0.EnhancedFix">
   ```

   b. Replace ***installationDirectory*** with the location where you installed IBM Business Monitor.

   c. Replace ***logLocation*** with the location and file name to log the information.

   For example:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\tools>imcl uninstall 8.0.0.0-WS-BPMADVWESB-IFJR39658
   -installationDirectory C:\IBM\BPM80 -log logfix.txt
   ```

The log (specified by the **-log** parameter) contains no error messages if uninstalling is successful. The command line shows a message that the fix was uninstalled.

# Chapter 13. Uninstalling IBM Business Monitor

You can remove IBM Business Monitor interactively or silently.

## Uninstalling IBM Business Monitor interactively

The Uninstall option in the Installation Manager enables you to uninstall packages from a single installation location. You can also uninstall all the installed packages from every installation location.

To uninstall the packages, you must log in to the system using the same user account that you used to install the product packages. A package cannot be uninstalled when another package has a dependency on it, unless the dependent package is also selected to be uninstalled.

1. Close the programs that you installed using Installation Manager.
2. Stop all running servers.
3. Display the Uninstall Packages page of the Installation Manager.
   - Start the Installation Manager. On the Start page, click **Uninstall**.
4. On the Uninstall Packages page, select IBM Business Monitor and associated packages that you want to uninstall.

   **Tip:** Windows If you started Installation Manager from the Start menu (**Start** > **...** > **Uninstall**) in the previous step, your IBM Business Monitor edition is pre-selected for uninstallation on the Uninstall Packages page.
   If you no longer need to use DB2 Express, or intend to reinstall IBM Business Monitor, select the **IBM DB2 Express** option to uninstall DB2 Express.**CAUTION:**
   **Only select the option to uninstall DB2 Express if you are sure that no other product is using DB2 Express. Selecting this option will delete all the DB2 Express databases and database assets even if other products, including products on a remote system, might use DB2 Express on this system.**
5. Click **Next**.
6. On the Summary page, review the list of packages that will be uninstalled, and then click **Uninstall**. After the uninstallation finishes, the Complete page opens.
7. Click **Finish** to exit the wizard.

When IBM Business Monitor is uninstalled, all profiles that are augmented to IBM Business Monitor are removed, including any WebSphere Application Server profiles that are augmented to IBM Business Monitor. For stand-alone monitor server profiles, the IBM Cognos BI service is removed.

Sample monitor models are not uninstalled to ensure that customizations of the models are preserved. To uninstall these models, see Removing monitor models and data.

If you plan to reinstall IBM Business Monitor, check for database issues that might affect the reinstallation procedure. Complete any action required before reinstalling the product:

- If databases were created in the previous install, ensure that the databases were dropped. See Reinstallation cannot create new profile.
- If you uninstalled DB2 Express, ensure that the BPMINST directory was deleted.
- If you uninstalled DB2 Express, delete the remaining DB2 Express entries in the `/etc/service` file. This is necessary because the new installation requires that port `50000` be available. Update the following file to remove any references to DB2 Express and port `50000`.

  Linux /etc/services

  Windows C:\Windows\System32\drivers\etc\services

© Copyright IBM Corp. 2005, 2012

For example, remove the following lines:

```
db2c_bpminst 50000/tcp
```

or

```
db2c_db2inst1 50000/tcp
```

## Uninstalling IBM Business Monitor silently

You can use the command-line mode of the Installation Manager to uninstall IBM Business Monitor.

Close all programs that you installed using the Installation Manager.

To uninstall, you must log in to the system using the same user account that you used to install.

To silently uninstall IBM Business Monitor, complete the following steps:

1. Open a command prompt, and change directories to the `/eclipse/tools` directory under Installation Manager.

   **Important:** If you are running Windows 7, Windows Vista, or Windows Server 2008, start your command prompt by right-clicking and selecting **Run as administrator**.
2. Make the appropriate replacements and run the following command:

   ```
   imcl uninstall list_of_product_IDs -installationDirectory installationDirectory -log logLocation
   -properties optionalProperties
   ```

   a. Replace ***list_of_product_IDs*** with a list of the IDs for the products you want to uninstall, separated by spaces.

      **Important:** The DB2 Express installation might be used by multiple products, including products on a remote system. If you uninstall DB2 Express, all DB2 Express databases and database assets are deleted.

*Table 9. Product IDs*

| Product | Product ID |
|---|---|
| IBM Business Monitor | com.ibm.websphere.MON.V80 |
| WebSphere Application Server Network Deployment | com.ibm.websphere.ND.v80 |
| Installation Manager | com.ibm.cic.agent |
| DB2 for Linux 32-bit | com.ibm.ws.DB2EXP97.linuxia32 |
| DB2 for Linux 64-bit | com.ibm.ws.DB2EXP97.linuxia64 |
| DB2 for Windows 32-bit | com.ibm.ws.DB2EXP97.winia32 |
| DB2 for Windows 64-bit | com.ibm.ws.DB2EXP97.winia64 |
| IBM Cognos Business Intelligence for Windows x86 (32-bit) | com.ibm.ws.cognos.v1011.winia32 |
| IBM Cognos BI for Windows x64 (64-bit) | com.ibm.ws.cognos.v1011.winia64 |
| IBM Cognos BI for AIX PPC 32-bit | com.ibm.ws.cognos.v1011.aix32 |
| IBM Cognos BI for AIX PPC 64-bit | com.ibm.ws.cognos.v1011.aix64 |
| IBM Cognos BI for Linux x86 (32-bit) | com.ibm.ws.cognos.v1011.linuxia32 |
| IBM Cognos BI for Linux x86-64 (64-bit) | com.ibm.ws.cognos.v1011.linuxia64 |
| IBM Cognos BI for Solaris SPARC (32-bit) | com.ibm.ws.cognos.v1011.solaris32 |
| IBM Cognos BI for Solaris SPARC (64-bit) | com.ibm.ws.cognos.v1011.solaris64 |
| IBM Cognos BI for Linux on System z | com.ibm.ws.cognos.v1011.zlinux64 |

b. Replace ***installationDirectory*** with the location where you installed the product.
c. Replace ***logLocation*** with the location and file name to log the information.

Installation Manager uninstalls the list of products and writes a log file to the directory that you specified.

The following example uninstalls IBM Business Monitor, WebSphere Application Server ND, and DB2 Express from Windows.

```
C:\Program Files\IBM\Installation Manager\eclipse\tools>imcl uninstall com.ibm.websphere.MON.V80
com.ibm.websphere.ND.v80 com.ibm.ws.cognos.v1011.winia32 com.ibm.ws.DB2EXP97.winia32
-installationDirectory C:\IBM\MON80 -log uninstalllog.txt
```

## Removing the showcase model

IBM Business Monitor comes with a mortgage lending showcase model that illustrates some of the functionality of IBM Business Monitor. You can install this model using First Steps.

To remove the showcase model:

1. Delete the Better Lender dashboard using the Space Manager.
2. Use the WebSphere Application Server administrative console to remove the alert templates.
3. If you have security enabled, remove the user role in the WebSphere Application Server administrative console.
4. Purge the model using the WebSphere Application Server administrative console.