

IBM InfoSphere Optim
Version 2 Release 2 Modification 3

*Configuring IBM Optim solution
components*



IBM InfoSphere Optim
Version 2 Release 2 Modification 3

*Configuring IBM Optim solution
components*



Note

Before using this information and the product it supports, read the information in "Notices" on page 33.

Version 2 Release 2 Modification 3 (November 2011)

This edition applies to version 2, release 2, modification 3 of IBM Optim solution components and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2008, 2011.

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

Contents

Tables	v
-------------------------	----------

About this publication	vii
---	------------

Chapter 1. InfoSphere Optim solution components 1

Optim Manager	1
Optim Management Server	1
Registry and repository	1
Optim Proxy	2
Optim Executor	2
Other service execution components	2
Optim Service Publisher	3
How services in a registry are run by using the manager and other components	3

Chapter 2. Configuring the manager and other components 5

Security for the manager	7
User roles in the manager	7
Configuring the manager and management server on WebSphere Application Server Community Edition	9
Deploying the management server WAR file on WebSphere Application Server Community Edition	9
Configuring the management server on WebSphere Application Server Community Edition	11

Deploying the manager WAR file on WebSphere Application Server Community Edition	17
Adding a user account for the manager on WebSphere Application Server Community Edition	19
Configuring the manager and management server on WebSphere Application Server	20
Deploying the management server WAR file on WebSphere Application Server v7.0	20
Deploying the manager WAR file on WebSphere Application Server v7.0	22
Configuring the proxy	23
Configuring the proxy as a Windows service	27
Configuring the proxy as a daemon on an AIX computer	27
Configuring the proxy as a daemon on a Linux computer	28
Configuring the proxy as a daemon on a Solaris computer	29
Configuring the executor	29
Adding a trust relationship between a management server and a proxy	30

Notices 33

Trademarks	35
----------------------	----

Index 37

Tables

- | | | | |
|----|--|----|--|
| 1. | User roles supported by the manager 7 | 4. | Service monitoring tasks that can be performed
by users with each security role 9 |
| 2. | Configuration and preference tasks that can be
performed by users with each security role . . 8 | | |
| 3. | Service management tasks that can be
performed by users with each security role . . 9 | | |

About this publication

This document describes how to configure IBM® Optim™ components so that the components can run IBM InfoSphere® Optim services that are located in a registry.

Chapter 1. InfoSphere Optim solution components

Use IBM InfoSphere Optim solution components to run InfoSphere Optim services that are published to a registry. Use IBM Optim Designer to develop and test InfoSphere Optim services. When you are done developing a service, you can publish the service to a registry for further testing or for production use.

Optim Manager

IBM Optim Manager is a web application that you can use to configure, run, monitor, and manage services. You also use Optim Manager to configure the components that are used to run these services. Optim Manager is also known as the *manager*.

To run services that you develop with IBM Optim Designer, access the manager through Optim Designer. (Optim Designer is also known as the *designer*.) When you are done developing the service, use the manager to publish the service to a registry. Alternatively, use the manager to export the service to the file system.

To run and manage services that have been published to a registry, access the manager through an application server. The manager is delivered as a web archive (WAR) file that you can deploy to any supported application server. For example, you can deploy the manager to WebSphere® Application Server Community Edition. You can then access the manager on the application server and use the manager to run and manage services in the registry of your choice.

You can deploy the management server WAR file and the manager WAR file either to the same application server or to separate application servers.

Optim Management Server

IBM Optim Management Server is a web application that manages and monitors service requests for services in a registry and repository. Optim Management Server can also host a registry and repository. Optim Management Server is also known as the *management server*.

The management server is delivered as a web archive (WAR) file that you can deploy to any supported application server. For example, you can deploy the management server to WebSphere Application Server Community Edition. You can deploy the management server and the manager either to the same application server or to separate application servers.

Registry and repository

The *registry* is a subsystem where services and other resources are enrolled. The registry is used to locate the services and resources. The *repository* is a persistent storage area for data and other application resources.

The registry and repository are installed with the management server and reside on the same computer as the management server.

Optim Proxy

IBM Optim Proxy is a constantly running process that receives service requests from the management server and forwards the service requests for processing. Optim Proxy monitors the running service requests until the service requests are complete. Optim Proxy is also known as the *proxy*.

The component to which the proxy forwards a service request depends upon the type of service.

- For some types of services, the proxy might start an instance of the component on the proxy computer. (For example, when the proxy receives an executor service request, the proxy starts an executor instance on the proxy computer.) For faster processing of these services, install the proxy on a computer that has fast connections to the data sources that you are processing.
- For other types of services, the proxy forwards the service request to a service execution component on another computer. When the service request is complete, the proxy returns the status of the service request to the manager and the management server.

Optim Executor

IBM Optim Executor is a process that runs services that specify the executor as their service execution component (service type of **Executor**). Optim Executor provides the framework needed by the service to communicate with a database or with any other type of resource needed by the service. Optim Executor is also known as the *executor*.

Services that specify the executor as their service execution component are also known as *data management services*.

When you run or execute a service, an instance of the executor is launched, and the executor processes the service. When the executor completes a service, the executor reports to the component that launched the executor that the service is complete. The executor then ends.

The executor is installed on the same computer as the designer or the proxy.

To run a service that uses lookup data, ensure that the executor has access to the lookup data. Load the lookup data into a database on the executor computer or on a computer that has a fast connection to the executor computer.

Related concepts

Chapter 2, “Configuring the manager and other components,” on page 5

In a production environment, the manager and other components in your Optim solution can be installed on different computers for greater performance and reliability. Configuring the components to work together might require the cooperation of many different people.

“Other service execution components”

Some types of services might require a service execution component other than the executor. For example, a service might be developed to run on Optim on distributed platforms.

Other service execution components

Some types of services might require a service execution component other than the executor. For example, a service might be developed to run on Optim on distributed platforms.

You might need to configure the designer or the proxy to run services that use these other service execution components. For information about how to configure the designer to run services that use a specific service execution component, see the designer user information. For information about how to configure the proxy to run services that use a specific service execution component, see the proxy configuration information.

Related concepts

Chapter 2, “Configuring the manager and other components,” on page 5

In a production environment, the manager and other components in your Optim solution can be installed on different computers for greater performance and reliability. Configuring the components to work together might require the cooperation of many different people.

“Optim Executor” on page 2

IBM Optim Executor is a process that runs services that specify the executor as their service execution component (service type of **Executor**). Optim Executor provides the framework needed by the service to communicate with a database or with any other type of resource needed by the service. Optim Executor is also known as the *executor*.

Optim Service Publisher

IBM Optim Service Publisher is a command-line utility that generates services from requests in an Optim Directory and publishes the services to a registry. After the services are generated and published, you can use the manager to run the services. (Optim Service Publisher is also known as the *publisher*.)

You can use the publisher to generate a service for an individual request in an Optim Directory. You can also use the publisher to generate services for many requests at a time.

When the publisher generates a service, the service is set to run with the parameters from the original Optim request in the Optim Directory. To change the parameters that are used by a publisher service, you must change the parameters in the original Optim request. You cannot use the manager to change the parameters that are used by a publisher service.

How services in a registry are run by using the manager and other components

Components must work together to complete a service request successfully.

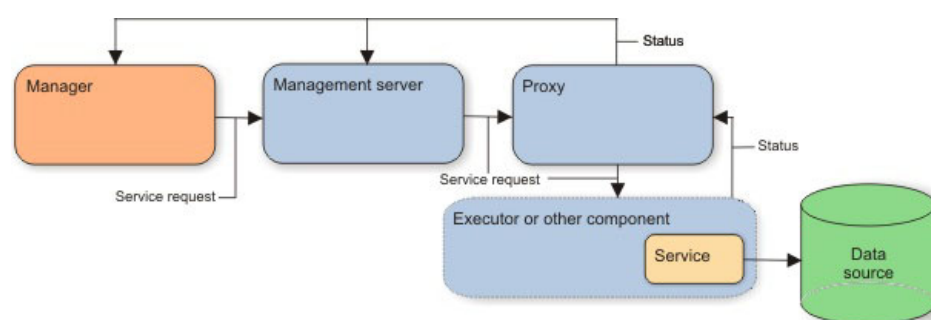


Figure 1. Components running a service

This diagram shows how components work together to run a service:

1. The application server administrator starts the management server and the manager, and the administrator of the proxy computer starts the proxy. The management server, the proxy, and the manager are designed to run continuously.
2. An operator uses the manager to run or schedule a service.
3. The manager sends the service request to the management server to which the service is assigned.
4. The management server forwards the service request to the proxy to which the service is assigned.

5. The proxy starts the service by using the component specified in the service. For services that the executor runs, the proxy starts an instance of the executor to process the service request. For services that another component runs, the proxy passes the service request to that component.
6. The executor or the other service execution component runs the service.
7. The service performs the tasks in its service plan.
8. For services that are run by the executor, the proxy continuously monitors the executor while the executor runs the service.
9. When the service is complete, the executor or the component that ran the service returns the service request status to the proxy. The executor instance also closes itself.
10. The proxy returns the service request status to the management server and the manager.

Chapter 2. Configuring the manager and other components

In a production environment, the manager and other components in your Optim solution can be installed on different computers for greater performance and reliability. Configuring the components to work together might require the cooperation of many different people.

The people who collaborate to configure the manager with other components might include:

- Application server administrator
- System administrator of proxy computer
- Service developer
- User with administrator access to the manager
- User with database administrator access to the manager

Application server administrator

The application server administrator is responsible for the initial setup of the manager and the management server. To complete the initial setup of the manager and the management server, the application server administrator must complete the following tasks:

1. Install the manager and management server by using IBM Installation Manager.

You can use Installation Manager to install a version of IBM WebSphere Application Server Community Edition that is delivered with the manager. You can deploy the manager and management server to WebSphere Application Server Community Edition for test and evaluation purposes.

2. Start the application server to which you will deploy the manager and the management server, if it is not already started.

3. Create a data source (or database pool) on the application server to which you will deploy the management server. Use `OptimServerDB` as the database name for this data source.

This data source is preconfigured when you install the version of WebSphere Application Server Community Edition that is delivered with the manager.

4. Create a data source (or database pool) on the application server to which you will deploy the manager. Use `optimConsoleDB` as the database name for this data source.

This data source is preconfigured when you install the version of WebSphere Application Server Community Edition that is delivered with the manager.

5. Deploy the management server and manager web archive (WAR) files to the application server.

If you are upgrading, remove any previous versions of the management server and manager WAR files before deploying the new versions of the WAR files.

The WAR files are in the following locations, where *shared_installation_directory* is the installation directory that you specified for the IBM Optim Shared package group.

- WAR file for the manager: *shared_installation_directory/console/app/optim.war*
- WAR file for the management server: *shared_installation_directory/server/app/management-server.war*

For example, the default location for the manager WAR file on Microsoft Windows is `C:\Program Files\IBM Optim\shared\console\app\optim.war`.

If you are upgrading, you must notify users that the manager is upgraded. A user might need to refresh the browser or clear the browser cache to get the upgraded version of the manager.

6. Configure user accounts for the manager.

A security realm called `optimConsoleRealm` is preconfigured when you install the version of WebSphere Application Server Community Edition that is delivered with the manager. The preconfigured `optimConsoleRealm` security realm stores security information in the `OOB_ROLE`, `OOB_USER`, and `OOB_USER_ROLE` tables in the `optimConsoleDB` database. You can add accounts, remove accounts, or change passwords by changing the user information in the `OOB_USER` and `OOB_USER_ROLE` tables.

7. To establish a secure connection between a management server and a proxy that are on separate computers, add a trust relationship between the management server and the proxy. You might need to work with the system administrator of the proxy computer to add this trust relationship.
8. If the executor is to be used to run services, create and configure replacement data and sample data tables on the database of your choice.

You can use Installation Manager to install the Optim Replacement Data Database with the management server. Alternatively, you can install the data from the Optim Replacement Data Database in comma-separated format. The data is installed with Data Definition Language (DDL) code. Use the DDL code to create and configure the replacement data and sample data tables on the database of your choice.

Depending on your needs, the application server administrator might choose to deploy additional instances of the management server and manager on other application servers.

System administrator of proxy computer

The system administrator is responsible for the initial setup of the proxy and of any service execution components that are used by the proxy. To complete the initial setup of the components, the system administrator must complete the following tasks:

1. Install the proxy by using Installation Manager.
2. Install the service execution component or components that are included with your solution. For example, if your solution includes the executor, install the executor by using Installation Manager.
3. Configure the proxy to use the service execution component or components that are included with your solution.
4. To establish a secure connection between a management server and a proxy that are on separate computers, add a trust relationship between the management server and the proxy. You might need to work with the administrator of the application server on which the management server is deployed to add this trust relationship.

Depending on your needs, the system administrator might choose to install additional instances of the proxy and the service execution component on other computers.

Service developer

A service developer is responsible for publishing services to the repository and testing services by using the manager. Service developers use IBM Optim Designer to design services, perform initial tests on the services, and publish services to a repository. The service developer can use the manager (user role designer) to verify that the service is on the repository and to test the service further. When the service developer is done testing, the service developer can promote the service to another repository.

For example, an enterprise uses a test repository and a production repository. A service developer at that enterprise uses Optim Designer to design services and publish the services to the test repository. The service developer then tests the services in the test repository. When the service is ready for production use, the service developer promotes the services to the production repository.

For more information about how to design, test, and publish services by using Optim Designer, see the Optim Designer documentation.

User with administrator access to the manager

Users with administrator access to the manager (user role admin) are responsible for configuring connections between the manager and the other components. An administrator must complete the following tasks:

1. Set the registry location.
2. Add management servers and proxies to the manager.

If the executor is to be used to run services, the administrator must also add a license to a management server.

User with database administrator access to the manager

If the executor is to be used to run services, users with database administrator access to the manager (user role dba) are responsible for adding database drivers to the repository.

Security for the manager

Security for the manager depends upon the environment from which you launch the manager. When you deploy the manager to an application server, security for the manager depends upon the security settings of the application server. When you launch the manager from the designer, you can run, publish, or export any service within the designer workspace to any available registry.

When you deploy the manager to an application server, use the application server to set up user authentication for the manager. The manager can use any authentication method that is supported by the application server. Regardless of the authentication method that you use on the application server, you must use the roles that are supported by the manager.

User roles in the manager

When you deploy the manager to an application server, the manager uses a predefined set of user roles. User roles define the tasks that each user can perform. Although user credentials are set up in the application server, the user credentials must use the roles that are supported by the manager.

Supported user roles

The manager supports the user roles that are listed in the following table. The administrator of the application server must map roles to user credentials so that users can sign onto the manager.

Table 1. User roles supported by the manager

Role ID	Role name	Description of role
0	admin	The administrator of the manager, who is responsible for configuring the management servers, proxies, and services.
1	dba	The database administrator, who is responsible for ensuring that the runtime environment has the resources needed to run the service against a database.
2	lob	The line-of-business administrator, who is responsible for ensuring that the service is performing its intended function.

Table 1. User roles supported by the manager (continued)

Role ID	Role name	Description of role
3	designer	The service designer, who is responsible for creating and testing services and for publishing services to the repository.
4	operator	The operator, who is responsible for scheduling and running services that are in the repository.

Assigning multiple user roles to a user

You can assign more than one user role to a single user. Each user role that you assign to a user gives the user access to the functions that are associated with the user role. For example, you assign the lob user role and the dba user role to a single user. For such a user, the user has access to the functions that are associated with both user roles.

User roles and users of external systems

For some product solutions, the manager might support the creation of user accounts that are based on user accounts on an external system. These product solutions might require you to create user accounts in this way to use the integration between the manager and the external system. When you use the manager to create such a user, you can assign any combination of user roles to the user.

Other elements of security

User roles are only one element of security that is provided by the manager. If a service is added to a service group, a user must be granted access to the service group before the user can run the service. Also, an administrator can configure tabs so that the tabs cannot be accessed by users who do not have a user role of admin. In these cases, a user might not be able to perform tasks that would otherwise be allowed by the user role.

Tasks

Each user role gives users permission to perform a set of tasks that are appropriate to users with that user role. The following tables indicate which tasks can be performed by users that have each user role.

Table 2. Configuration and preference tasks that can be performed by users with each security role

Tasks	Roles
View Management Servers, Proxies, and Database Drivers on the Configuration tab	admin, dba, lob, designer, operator
View Users and Groups and Tabs on the Configuration tab	admin
Set registry location and global preferences	admin
Set user and display preferences	admin, dba, lob, designer, operator
Manage management servers and proxies	admin
Manage licenses for management servers	admin, dba
Manage database drivers in the repository	admin, dba
Manage service groups	admin
Grant and remove user access to service groups	admin

Table 2. Configuration and preference tasks that can be performed by users with each security role (continued)

Tasks	Roles
Manage manager user accounts for users of external systems	admin
Manage user-defined tabs	admin
Change access to tabs in the manager	admin

Table 3. Service management tasks that can be performed by users with each security role

Tasks	Roles
View the Service Management tab	admin, dba, lob, designer, operator
Run services and service sets	admin, dba, lob, designer, operator
Schedule services and service sets	admin, dba, designer, operator
Change service plan	admin, dba, designer, operator
Manage service sets	admin, dba, lob, designer, operator
Reassign services to a different management server and proxy	admin, dba, operator
Import a service	admin, dba
Export a service	admin, dba, operator
Promote a service	admin, dba

Table 4. Service monitoring tasks that can be performed by users with each security role

Tasks	Roles
View the Dashboard and Service Monitoring tabs	admin, dba, lob, designer, operator
Stop services	admin, dba, lob, designer, operator
Purge service instance information	admin, dba
Manage service instance filters	admin, dba

Configuring the manager and management server on WebSphere Application Server Community Edition

The tasks that you must perform to configure the manager and the management server depend upon the application server that you use. The manager is delivered with a version of WebSphere Application Server Community Edition that is preconfigured for use with the manager and management server. This version of WebSphere Application Server Community Edition allows you to install and configure the manager and management server more quickly and easily for evaluation purposes.

The version of WebSphere Application Server Community Edition that is delivered with the manager is available only in English. You must configure this version of WebSphere Application Server Community Edition by using an English user interface. However, when you use the manager, the language setting of the browser determines the language of the manager user interface. The language setting of the browser also determines the language of the messages that are received from the management server and proxy.

Deploying the management server WAR file on WebSphere Application Server Community Edition

You can use IBM Installation Manager to install the management server and its associated databases and data files to an application server computer. However, installation is not complete until you deploy the

management server Web archive (WAR) file to the application server. Use this task to deploy the management server WAR file on the English version of WebSphere Application Server Community Edition.

When you deploy the management server WAR file to the application server, the application server creates an Apache Derby database called OptimServerDB.

The version of WebSphere Application Server Community Edition that is delivered with the manager is available only in English. You must configure this version of WebSphere Application Server Community Edition by using an English user interface. However, when you use the manager, the language setting of the browser determines the language of the manager user interface. The language setting of the browser also determines the language of the messages that are received from the management server and proxy.

Use the Administrative Console of WebSphere Application Server Community Edition to deploy the management server WAR file. The default location of the administrative console is `http://hostname:8080/console`, where *hostname* is the host name of the computer on which WebSphere Application Server Community Edition is installed.

To deploy the management server WAR file by using the Administrative Console of WebSphere Application Server Community Edition:

1. Click **Deploy New**.
2. Enter the location of the management server WAR file into **Archive**, and click **Install**. The management server WAR file is `shared_installation_directory/server/app/management-server.war`, where *shared_installation_directory* is the installation directory that you specified for the IBM Optim Shared package group. For example, the default location for the management server WAR file on Microsoft Windows is `C:\Program Files\IBM Optim\shared\server\app\management-server.war`. If you prefer, you can click **Browse** to browse for the management server WAR file. The management server WAR file can take several minutes to deploy.

After you deploy the management server WAR file, you can configure management server properties by editing the application server startup script. This script is located at the following location, where *shared_installation_directory* is the installation directory that you specified for the Optim Management Server installation package.

- Windows computers: `shared_installation_directory\WebSphere\AppServerCommunityEdition\bin\startup.bat`
- Linux or UNIX computers: `shared_installation_directory\WebSphere\AppServerCommunityEdition\bin/startup.sh`

If the WAR file fails to deploy because of `java.lang.OutOfMemoryError: PermGen space` errors, increase the amount of permanent generation memory available for objects in the Java Virtual Machine (VM) on the application server. To increase the available amount of permanent generation memory, edit the application server startup script. Open this script in a text editor and add the following argument to the end of the `JAVA_OPTS` parameter in the script. *NNN* is the initial amount of permanent generation memory in MB and *MMM* is the maximum amount of permanent generation memory in MB. The entire `JAVA_OPTS` parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-XX:PermSize=NNNm -XX:MaxPermSize=MMMm
```

For example, the following `JAVA_OPTS` parameter from a Windows batch script specifies 128 MB as the initial amount of permanent generation memory and 256 MB as the maximum amount of permanent generation memory.

```
@set JAVA_OPTS=%ADDITIONAL_JAVA_OPTS% %JAVA_OPTS% ^
-Djavax.net.ssl.keyStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.trustStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager ^
-XX:PermSize=128m -XX:MaxPermSize=256m
```

The following `JAVA_OPTS` parameter from a Linux or UNIX script specifies 128 MB as the initial amount of permanent generation memory and 256 MB as the maximum amount of permanent generation memory.

```
JAVA_OPTS=-Djavax.net.ssl.keyStore=$GHOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.trustStore=$GHOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager \
-XX:PermSize=128m -XX:MaxPermSize=256m \
$JAVA_OPTS
```

By default, the management server uses 64 MB of permanent generation memory. Setting memory sizes to a value larger than the amount of available physical memory on your machine severely degrades performance.

If the application server is on a computer that is set to a language that requires the use of double-byte characters, configure the application server to use UTF-8 encoding in its log files. To configure the application server to use UTF-8 encoding, add the following argument to the end of the `JAVA_OPTS` parameter in the application server startup script. The entire `JAVA_OPTS` parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-Dfile.encoding=UTF-8
```

If the WAR file fails to deploy to a Linux computer because of `IOException: too many open files` errors, increase the maximum number of open files on the computer. To increase the maximum number of open files, sign on as superuser and complete the following steps.

1. Enter the following command:

```
/sbin/sysctl -w fs.file-max=100000
```
2. Add the following line to the `/etc/sysctl.conf` file so that the setting remains as it is after system reboot.

```
fs.file-max = 100000
```
3. Enter the following command so that the change to the `/etc/sysctl.conf` file takes effect.

```
/sbin/sysctl -p
```
4. Enter the following command to verify the settings.

```
/sbin/sysctl fs.file-max
```
5. Enter the following command to increase the maximum number of processes to 20,048.

```
ulimit -n 20048
```
6. Add the following line to the beginning of the `shared_installation_directory/WebSphere/AppServerCommunityEdition/bin/startup.sh` script so that the setting is set every time that you start the application server.

```
ulimit -n 20048
```

Configuring the management server on WebSphere Application Server Community Edition

After you deploy the management server to WebSphere Application Server Community Edition, you can configure management server properties. To configure management server properties, edit the script that you use to start WebSphere Application Server Community Edition.

Location of startup script

When you install WebSphere Application Server Community Edition with the management server, Installation Manager automatically creates a startup script for WebSphere Application Server Community Edition. The startup script is located at the following location, where *shared_installation_directory* is the installation directory that you specified for the Optim Management Server installation package.

- Windows computers: *shared_installation_directory*\WebSphere\AppServerCommunityEdition\bin\startup.bat
- Linux or UNIX computers: *shared_installation_directory*/WebSphere/AppServerCommunityEdition/bin/startup.sh

Setting the registry and repository locations

If you use more than one management server, each management server has its own registry and repository. To use a single registry and repository for all management servers, you must choose one management server to act as the registry and repository. You can then set all other management servers to use that registry and repository. To set a management server to use a registry and repository, add the following arguments to the JAVA_OPTS parameter in the startup script. The entire JAVA_OPTS parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-Dcom.ibm.optim.registry.url=registry_URL  
-Dcom.ibm.optim.repository.url=repository_URL
```

- *registry_URL* is the location of the registry.
- *repository_URL* is the location of the repository.

For example, the following JAVA_OPTS parameter from a Windows batch script specifies `http://mgmtserver1:8080/server/registry` as the registry location and `http://mgmtserver1:8080/server/repository` as the repository location.

```
@set JAVA_OPTS=%ADDITIONAL_JAVA_OPTS% %JAVA_OPTS% ^  
-Djavax.net.ssl.keyStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^  
-Djavax.net.ssl.trustStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^  
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager ^  
-Dcom.ibm.optim.registry.url=http://mgmtserver1:8080/server/registry ^  
-Dcom.ibm.optim.repository.url=http://mgmtserver1:8080/server/repository
```

The following JAVA_OPTS parameter from a Linux or UNIX script specifies `http://mgmtserver1:8080/server/registry` as the registry location and `http://mgmtserver1:8080/server/repository` as the repository location.

```
JAVA_OPTS=-Djavax.net.ssl.keyStore=$GHOME/./var/security/keystores/optim-management-server.jks \  
-Djavax.net.ssl.trustStore=$GHOME/./var/security/keystores/optim-management-server.jks \  
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager \  
-Dcom.ibm.optim.registry.url=http://mgmtserver1:8080/server/registry \  
-Dcom.ibm.optim.repository.url=http://mgmtserver1:8080/server/repository \  
$JAVA_OPTS
```

If you assign IP addresses dynamically to computers, use the host name of the computer that hosts the registry and repository instead of the IP address.

Setting the host name and port for a management server

If you assign IP addresses dynamically to computers, or if the application server uses a port number other than 8080, set the host name and port that are used by the management server. To set the host name and port for the management server, add the following arguments to the JAVA_OPTS parameter in the startup script. The entire JAVA_OPTS parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.


```
-Dcom.ibm.optim.host.name=host_name
-Dcom.ibm.optim.host.port=host_port
```

- *host_name* is the host name or IP address of the management server.
- *host_port* is the port used by the management server.

For example, the following JAVA_OPTS parameter from a Windows batch script specifies mgmtserver as the host name of the management server and 8080 as the port number used by the management server.

```
@set JAVA_OPTS=%ADDITIONAL_JAVA_OPTS% %JAVA_OPTS% ^
-Djavax.net.ssl.keyStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.trustStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager ^
-Dcom.ibm.optim.host.name=mgmtserver ^
-Dcom.ibm.optim.host.port=8080
```

The following JAVA_OPTS parameter from a Linux or UNIX script specifies mgmtserver as the host name of the management server and 8080 as the port number used by the management server.

```
JAVA_OPTS=-Djavax.net.ssl.keyStore=$HOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.trustStore=$HOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager \
-Dcom.ibm.optim.host.name=mgmtserver \
-Dcom.ibm.optim.host.port=8080 \
$JAVA_OPTS
```

Setting the management server to use the https protocol

As one step in establishing a trust relationship between a management server and a proxy, you must set the management server to use the https protocol to communicate with other components. The management server uses the http protocol unless you set the management server to use the https protocol. To set the management server to use the https protocol, add the following argument to the JAVA_OPTS parameter in the startup script. The entire JAVA_OPTS parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-Dcom.ibm.optim.url.protocol=https
```

If a management server uses the https protocol, you must also set the registry and repository locations to use the https protocol.

For example, the following JAVA_OPTS parameter from a Windows batch script specifies https://mgmtserver1:8080/server/registry as the registry location and https://mgmtserver1:8080/server/repository as the repository location.

```
@set JAVA_OPTS=%ADDITIONAL_JAVA_OPTS% %JAVA_OPTS% ^
-Djavax.net.ssl.keyStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.trustStore="%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager ^
-Dcom.ibm.optim.registry.url=https://mgmtserver1:8080/server/registry ^
-Dcom.ibm.optim.repository.url=https://mgmtserver1:8080/server/repository ^
-Dcom.ibm.optim.url.protocol=https
```

The following JAVA_OPTS parameter from a Linux or UNIX script specifies https://mgmtserver1:8080/server/registry as the registry location and https://mgmtserver1:8080/server/repository as the repository location.

```
JAVA_OPTS=-Djavax.net.ssl.keyStore=$HOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.trustStore=$HOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager \
-Dcom.ibm.optim.registry.url=https://mgmtserver1:8080/server/registry \
-Dcom.ibm.optim.repository.url=https://mgmtserver1:8080/server/repository \
-Dcom.ibm.optim.url.protocol=https \
$JAVA_OPTS
```

Configuring the management server as a Windows service

If you deploy the management server to WebSphere Application Server Community Edition on Microsoft Windows, you can configure the management server as a Windows service. You can set the management server service to restart automatically whenever the computer is restarted.

Before you begin, install and deploy the management server to WebSphere Application Server Community Edition.

The computer must have Microsoft .NET Framework 2.0 or higher installed.

To configure the management server as a Windows service:

1. If WebSphere Application Server Community Edition is not installed to the default location at C:\Program Files\IBM Optim\shared\WebSphere\AppServerCommunityEdition, complete the following steps:
 - a. Open the folder in which you installed WebSphere Application Server Community Edition.
 - b. Open the bin folder, and then open the mgmtServerService.xml file in that folder by using a text editor such as Notepad.
 - c. Change the value of the wasceLocation entity to the folder in which you installed WebSphere Application Server Community Edition, and save the changed mgmtServerService.xml file.
 - d. Open the optimService.bat file in that folder by using a text editor such as Notepad.
 - e. Change the WASCE_BIN value to *server_location*\bin, where *server_location* is the folder in which you installed WebSphere Application Server Community Edition, and save the changed optimService.bat file.

For example, you install WebSphere Application Server Community Edition to D:\Applications\IBM Optim\WASCE. In this case, use Notepad to open D:\Applications\IBM Optim\WASCE\mgmtServerService.xml and change the wasceLocation value to D:\Applications\IBM Optim\WASCE. Next, open D:\Applications\IBM Optim\WASCE\optimService.bat and change the WASCE_BIN value to D:\Applications\IBM Optim\WASCE\bin. On computers that run a 64-bit version of Windows, WebSphere Application Server Community Edition is installed to C:\Program Files (x86)\IBM Optim\shared\WebSphere\AppServerCommunityEdition by default. You must therefore always edit the mgmtServerService.xml file on computers that run a 64-bit version of Windows.

2. If you configure WebSphere Application Server Community Edition to use a non-default user name, password, and port number, configure the service to use these values. By default, WebSphere Application Server Community Edition is configured to use system as the user name, manager as the password, and 1099 as the port number. Complete the following steps:
 - a. Open the folder in which you installed WebSphere Application Server Community Edition.
 - b. Open the bin folder, and then open the optimService.bat file in that folder by using a text editor such as Notepad.
 - c. Change the USER, PASSWORD, and PORT values to the values that you configured for WebSphere Application Server Community Edition.
3. Open the command prompt by clicking **Start > Run** and entering the command **cmd**.
4. Enter the following commands at the command prompt, where *server_location* is the location in which WebSphere Application Server Community Edition is installed:

```
cd server_location
mgmtServerService.exe install
mgmtServerService.exe start
```

You can check on the progress of the management server by looking at the contents of log files. There are 3 log files:

- *server_location*/log/mgmtServerService.err.log
- *server_location*/log/mgmtServerService.out.log
- *server_location*/log/mgmtServerService.wrapper.log

To stop and uninstall the management server service, enter the following commands at the command prompt.

```
cd server_location
mgmtServerService.exe stop
mgmtServerService.exe uninstall
```

Configuring the management server as a daemon on an AIX computer

If you deploy the management server to WebSphere Application Server Community Edition on AIX®, you can configure the management server to run as a daemon process. You can set the management server daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the management server as a daemon on an AIX computer:

1. Open the command prompt.
2. Enter the following commands at the command prompt, where *server_location* is the directory in which WebSphere Application Server Community Edition is installed:

```
cd server_location/bin
./setup-mgmtserver-as-daemon.sh
```

The script generates a script called *optimgmtserver*, which is saved to the *server_location/bin* directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script *optimgmtserver* to the */etc/rc.d/init.d* directory.
5. Enter the following commands at the command prompt.

```
cd /etc/rc.d/init.d
chmod 755 optimgmtserver
ln -s optimgmtserver /etc/rc.d/rc2.d/S99optimgmtserver
ln -s optimgmtserver /etc/rc.d/rc2.d/K01optimgmtserver
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/rc.d/init.d/optimgmtserver start
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/rc.d/init.d/optimgmtserver stop
```

To remove the management server daemon, log in as superuser and enter the following commands at the command prompt. Remove the management server daemon before you uninstall WebSphere Application Server Community Edition.

```
/etc/rc.d/init.d/optimgmtserver stop
rm /etc/rc.d/rc2.d/S99optimgmtserver
rm /etc/rc.d/rc2.d/K01optimgmtserver
rm /etc/rc.d/init.d/optimgmtserver
```

Configuring the management server as a daemon on a Linux computer

If you deploy the management server to WebSphere Application Server Community Edition on Linux, you can configure the management server to run as a daemon process. You can set the management server daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the management server as a daemon on a Linux computer:

1. Open the command prompt.
2. Enter the following commands at the command prompt, where *server_location* is the directory in which WebSphere Application Server Community Edition is installed:

```
cd server_location/bin
./setup-mgmtserver-as-daemon.sh
```

The script generates a script called `optimmgmtserver`, which is saved to the *server_location*/bin directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script `optimmgmtserver` to the `/etc/rc.d/init.d` directory.
5. Enter the following commands at the command prompt.

```
cd /etc/rc.d/init.d
chmod 755 optimmgmtserver
/sbin/chkconfig --add optimmgmtserver
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/sbin/service optimmgmtserver start
```

To view the init levels at which the daemon is started or stopped, log in as superuser and enter the following command at the command prompt.

```
/sbin/chkconfig --list optimmgmtserver
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/sbin/service optimmgmtserver stop
```

To remove the management server daemon, log in as superuser and enter the following commands at the command prompt. Remove the management server daemon before you uninstall WebSphere Application Server Community Edition.

```
/sbin/service optimmgmtserver stop
/sbin/chkconfig --del optimmgmtserver
rm /etc/rc.d/init.d/optimmgmtserver
```

Configuring the management server as a daemon on a Solaris computer

If you deploy the management server to WebSphere Application Server Community Edition on Solaris, you can configure the management server to run as a daemon process. You can set the management server daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the management server as a daemon on a Solaris computer:

1. Open the command prompt.
2. Enter the following commands at the command prompt, where *server_location* is the directory in which WebSphere Application Server Community Edition is installed:

```
cd server_location/bin
./setup-mgmtserver-as-daemon.sh
```

The script generates a script called `optimmgmtserver`, which is saved to the *server_location*/bin directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script `optimmgmtserver` to the `/etc/init.d` directory.
5. Enter the following commands at the command prompt.

```
cd /etc/init.d
chmod 755 optimmgmtserver
ln -s optimmgmtserver /etc/rc3.d/S99optimmgmtserver
ln -s optimmgmtserver /etc/rc3.d/K01optimmgmtserver
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/init.d/optimmgmtserver start
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/init.d/optimmgmtserver stop
```

To remove the management server daemon, log in as superuser and enter the following commands at the command prompt. Remove the management server daemon before you uninstall WebSphere Application Server Community Edition.

```
/etc/init.d/optimmgmtserver stop  
rm /etc/rc3.d/S99optimmgmtserver  
rm /etc/rc3.d/K01optimmgmtserver  
rm /etc/init.d/optimmgmtserver
```

Deploying the manager WAR file on WebSphere Application Server Community Edition

You must deploy the manager Web archive (WAR) file to the application server before you can use the manager. Use this task to deploy the WAR file on the English version of WebSphere Application Server Community Edition.

When you deploy the WAR file to the application server, the application server creates an Apache Derby database called `optimConsoleDB`. The application server associates the `optimConsoleDB` database with the `OptimConsoleDB` database pool.

The version of WebSphere Application Server Community Edition that is delivered with the manager is available only in English. You must configure this version of WebSphere Application Server Community Edition by using an English user interface. However, when you use the manager, the language setting of the browser determines the language of the manager user interface. The language setting of the browser also determines the language of the messages that are received from the management server and proxy.

Use the Administrative Console of WebSphere Application Server Community Edition to deploy the WAR file. The default location of the Administrative Console is `http://hostname:8080/console`, where *hostname* is the host name of the computer on which WebSphere Application Server Community Edition is installed.

To deploy the manager WAR file with the Administrative Console of WebSphere Application Server Community Edition:

1. Click **Deploy New**.
2. Enter the location of the WAR file into **Archive**, and click **Install**. The WAR file is `shared_installation_directory/console/app/optim.war`, where *shared_installation_directory* is the installation directory that you specified for the IBM Optim Shared package group. For example, the default location for the WAR file on Microsoft Windows is `C:\Program Files\IBM\Optim\shared\console\app\optim.war`. If you prefer, you can click **Browse** to browse for the WAR file. The WAR file can take several minutes to deploy.
3. If you are upgrading a manager WAR file, notify all users that you have deployed an upgraded version of the manager. A user might need to refresh the browser or clear the browser cache to get the upgraded version of the manager. A user can see whether the browser has the upgraded version of the manager by clicking **Help > About IBM Optim Manager** in the manager interface.

After you deploy the manager WAR file to the application server, you can configure manager properties. To configure manager properties, edit the script that you use to start the application server. This script is located at the following location, where *shared_installation_directory* is the installation directory that you specified for the Optim Manager installation package.

- Windows computers: `shared_installation_directory\WebSphere\AppServerCommunityEdition\bin\startup.bat`

- Linux or UNIX computers: *shared_installation_directory*/WebSphere/AppServerCommunityEdition/bin/startup.sh

If the WAR file fails to deploy because of java.lang.OutOfMemoryError: PermGen space errors, increase the amount of permanent generation memory available for objects in the Java Virtual Machine (VM) on the application server. To increase the available amount of permanent generation memory, edit the application server startup script. Open this script in a text editor and add the following argument to the end of the JAVA_OPTS parameter in the script. *NNN* is the initial amount of permanent generation memory in MB and *MMM* is the maximum amount of permanent generation memory in MB. The entire JAVA_OPTS parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-XX:PermSize=NNNm -XX:MaxPermSize=MMMm
```

For example, the following JAVA_OPTS parameter from a Windows batch script specifies 128 MB as the initial amount of permanent generation memory and 256 MB as the maximum amount of permanent generation memory.

```
@set JAVA_OPTS=%ADDITIONAL_JAVA_OPTS% %JAVA_OPTS% ^
-Djavax.net.ssl.keyStore=%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.trustStore=%GERONIMO_HOME%\var\security\keystores\optim-management-server.jks" ^
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager ^
-XX:PermSize=128m -XX:MaxPermSize=256m
```

The following JAVA_OPTS parameter from a Linux or UNIX script specifies 128 MB as the initial amount of permanent generation memory and 256 MB as the maximum amount of permanent generation memory.

```
JAVA_OPTS=-Djavax.net.ssl.keyStore=$GHOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.trustStore=$GHOME/./var/security/keystores/optim-management-server.jks \
-Djavax.net.ssl.keyStorePassword=manager -Djavax.net.ssl.trustStorePassword=manager \
-XX:PermSize=128m -XX:MaxPermSize=256m \
$JAVA_OPTS
```

By default, the manager uses 64 MB of permanent generation memory. Setting memory sizes to a value larger than the amount of available physical memory on your machine severely degrades performance.

If the application server is on a computer that is set to a language that requires the use of double-byte characters, configure the application server to use UTF-8 encoding in its log files. To configure the application server to use UTF-8 encoding, add the following argument to the end of the JAVA_OPTS parameter in the application server startup script. The entire JAVA_OPTS parameter must be either on a single line or on consecutive lines that are connected with line-continuation characters. The line-continuation character is the caret (^) for Windows batch scripts or the backslash (\) for Linux or UNIX scripts.

```
-Dfile.encoding=UTF-8
```

If the WAR file fails to deploy to a Linux computer because of IOException: too many open files errors, increase the maximum number of open files on the computer. To increase the maximum number of open files, sign on as superuser and complete the following steps.

1. Enter the following command:
/sbin/sysctl -w fs.file-max=100000
2. Add the following line to the /etc/sysctl.conf file so that the setting remains as it is after system reboot.
fs.file-max = 100000
3. Enter the following command so that the change to the /etc/sysctl.conf file takes effect.
/sbin/sysctl -p
4. Enter the following command to verify the settings.
/sbin/sysctl fs.file-max
5. Enter the following command to increase the maximum number of processes to 20,048.

```
ulimit -n 20048
```

6. Add the following line to the beginning of the *shared_installation_directory*/WebSphere/AppServerCommunityEdition/bin/startup.sh script so that the setting is set every time that you start the application server.

```
ulimit -n 20048
```

Adding a user account for the manager on WebSphere Application Server Community Edition

If you use the default user security configuration for the manager on WebSphere Application Server Community Edition, user security information is stored in a database. You can use SQL commands to maintain user accounts in this database. Use this task to create a user account on this database.

Use this topic to add user accounts for the manager only if you are using the default user security configuration for the manager. The default user security configuration might not be secure enough for production use.

For some product solutions, the manager might support the creation of user accounts that are based on user accounts on an external system. For these product solutions, create user accounts through the manager user interface so that you can fully use the integration with the external system. If you do not use such a product solution, create new user accounts by following the security environment that has been established for the application server.

Before you can add a user account, deploy the manager Web archive (WAR) file to WebSphere Application Server Community Edition.

The version of WebSphere Application Server Community Edition that is delivered with the manager is available only in English. You must configure this version of WebSphere Application Server Community Edition by using an English user interface. However, when you use the manager, the language setting of the browser determines the language of the manager user interface. The language setting of the browser also determines the language of the messages that are received from the management server and proxy.

Use the Administrative Console of WebSphere Application Server Community Edition to add a user account for the manager. The default location of the Administrative Console is `http://hostname:8080/console`, where *hostname* is the host name of the computer on which WebSphere Application Server Community Edition is installed.

To add a user account for the manager by using the Administrative Console of WebSphere Application Server Community Edition:

1. Click **DB Manager**.
2. In **Use DB**, select **optimConsoleDB**.
3. Enter the following SQL commands into **SQL Command/s**.

```
INSERT INTO CONSOLE2.00B_USER values(userid,username,password);  
INSERT INTO CONSOLE2.00B_USER_ROLE values(userid,roleid,rolename);
```

- The integer value *userid* uniquely identifies the user.
- The varchar value *username* specifies the user name. The user name is typically a string value.
- The varchar value *password* specifies the user password. The user password is typically a string value.
- The integer value *roleid* and the varchar value *rolename* are values that correspond with each user role ID and user role name:
 - The user role ID 0 and user role name admin correspond with the admin (manager administrator) user role.
 - The user role ID 1 and user role name dba correspond with the dba (database administrator) user role.

- The user role ID 2 and user role name lob correspond with the lob (line-of-business) user role.
- The user role ID 3 and user role name designer correspond with the designer user role.
- The user role ID 4 and user role name operator correspond with the operator user role.

4. Click **Run SQL**.

For example, the following SQL code creates a user ID with the admin user role and a user ID with the operator user role. Both user IDs use passw0rd as the password.

```
INSERT INTO CONSOLE2.OOB_USER values(10,'administrator','passw0rd');
INSERT INTO CONSOLE2.OOB_USER_ROLE values(10,0,'admin');
INSERT INTO CONSOLE2.OOB_USER values(11,'user14','passw0rd');
INSERT INTO CONSOLE2.OOB_USER_ROLE values(11,4,'operator');
```

Related tasks

“Deploying the manager WAR file on WebSphere Application Server Community Edition” on page 17
You must deploy the manager Web archive (WAR) file to the application server before you can use the manager. Use this task to deploy the WAR file on the English version of WebSphere Application Server Community Edition.

Related reference

“Security for the manager” on page 7

Security for the manager depends upon the environment from which you launch the manager. When you deploy the manager to an application server, security for the manager depends upon the security settings of the application server. When you launch the manager from the designer, you can run, publish, or export any service within the designer workspace to any available registry.

Configuring the manager and management server on WebSphere Application Server

The tasks that you must perform to configure the manager and management server depend upon the application server that you use. For enterprise use, you can choose to use WebSphere Application Server as your application server.

Deploying the management server WAR file on WebSphere Application Server v7.0

You can use IBM Installation Manager to install the management server and its associated databases and data files to an application server computer. However, installation is not complete until you deploy the management server Web archive (WAR) file to the application server. Use this task to deploy the management server WAR file on WebSphere Application Server.

Before you begin, install WebSphere Application Server. To avoid path length issues, avoid installing WebSphere Application Server into a long path. For example, if you install WebSphere Application Server to a Windows computer, C:\WAS70 is an acceptable installation location.

After you install WebSphere Application Server, start the instance of the Apache Derby database that is installed with WebSphere Application Server. To start the Derby database, complete the following, where *was_folder* is the folder in which WebSphere Application Server is installed.

- Windows: Run the *was_folder\derby\bin\networkServer\startNetworkServer.bat* batch file.
- AIX/Linux/Solaris: Run the *was_folder/derby/bin/networkServer/startNetworkServer* script.

Use the Integrated Solutions Console of WebSphere Application Server to deploy the WAR file. The default location of the administrative console is <http://hostname:9043/ibm/console>, where *hostname* is the host name of the computer on which WebSphere Application Server is installed.

To deploy the management server WAR file using the Integrated Solutions Console of WebSphere Application Server:

1. Click **Resources > JDBC > Data Sources** and create a data source with the following properties. Use the defaults for all other properties:

Step 1: Enter basic data source information

- **Data source name:** OptimServerDS
- **JNDI name:** jdbc/OptimServerDS

Step 2: Select JDBC provider

Select an existing JDBC provider: Derby Network Server Using Derby Client 40 (XA)

Step 3: Enter database specific properties for the data source

Database name: OptimServerDB;create=true

When you are done, click **Save** to save the data source, and then click **Test connection** to test the data source.

2. Click **Applications > New Application > New Enterprise Application** and deploy the WAR file with the following properties. Use the defaults for all other properties:

Preparing for the application installation

The management server WAR file is *shared_installation_directory/server/app/management-server.war*, where *shared_installation_directory* is the installation directory that you specified for the IBM Optim Shared package group. For example, the default location for the management server WAR file on Microsoft Windows is C:\Program Files\IBM Optim\shared\server\app\management-server.war. If you prefer, you can click **Browse** to browse for the file. Use **Fast Path** to install the application.

Step 3: Map resource references to resources

Click **Browse**, select **OptimServerDS** and click **Apply**.

Step 5: Map context roots for Web modules

Context Root: /server

The WAR file can take several minutes to deploy. When you are done, click **Save** to save the configuration.

3. Click **Applications > Application types > WebSphere enterprise applications > management-server_war > Class loading and update detection**, select **Classes loaded with local class loader first (parent last)**, click **Apply**, and click **Save**.
4. Click **Servers > Server types > WebSphere application servers > server1 > Java and Process Management > Process definition > Java Virtual Machine > Custom properties**, and add the following properties.

com.ibm.optim.host.name

The name of the host on which you have installed WebSphere Application Server.

com.ibm.optim.host.port

The port on which the web container is running. The default port is 9080.

com.ibm.optim.registry.url

The location of the registry. This is `http://hostname:port/server/registry`, where *hostname* is the value of `com.ibm.optim.host.name`, and *port* is the value of `com.ibm.optim.host.port`.

com.ibm.optim.repository.url

The location of the repository. This is `http://hostname:port/server/repository`, where *hostname* is the value of `com.ibm.optim.host.name`, and *port* is the value of `com.ibm.optim.host.port`.

When you are done, click **Save** to save the configuration.

5. Stop and restart WebSphere Application Server.

6. Click **Applications > Application types > WebSphere enterprise applications** and verify that **management-server_war** is running. If not, select the **Select** box for **management-server_war** and click **Start**. The application can take several minutes to start.

After you deploy the management server on WebSphere Application Server, you must configure the proxies to access the registry and repository on the management server.

Deploying the manager WAR file on WebSphere Application Server v7.0

You can use IBM Installation Manager to install the manager and its associated databases and data files to an application server computer. However, installation is not complete until you deploy the manager Web archive (WAR) file to the application server. Use this task to deploy the manager WAR file on WebSphere Application Server.

Before you begin, install WebSphere Application Server. To avoid path length issues, avoid installing WebSphere Application Server into a long path. For example, if you install WebSphere Application Server to a Windows computer, C:\WAS70 is an acceptable installation location.

After you install WebSphere Application Server, start the instance of the Apache Derby database that is installed with WebSphere Application Server. To start the Derby database, complete the following, where *was_folder* is the folder in which WebSphere Application Server is installed.

- Windows: Run the *was_folder\derby\bin\networkServer\startNetworkServer.bat* batch file.
- AIX/Linux/Solaris: Run the *was_folder/derby/bin/networkServer/startNetworkServer* script.

You must also use WebSphere Application Server to create the users and user groups that are to be used for the manager. During this task, you must map users and user groups in WebSphere Application Server to the user roles available for the manager. For more information about how to create users and user groups, see the documentation for WebSphere Application Server.

Use the Integrated Solutions Console of WebSphere Application Server to deploy the WAR file. The default location of the administrative console is <http://hostname:9043/ibm/console>, where *hostname* is the host name of the computer on which WebSphere Application Server is installed.

To deploy the manager WAR file by using the Integrated Solutions Console of WebSphere Application Server:

1. Click **Resources > JDBC > Data Sources** and create a data source with the following properties. Use the defaults for all other properties:

Step 1: Enter basic data source information

- **Data source name:** OptimConsoleDS
- **JNDI name:** jdbc/optimconsoleDS

Step 2: Select JDBC provider

Select an existing JDBC provider: Derby Network Server Using Derby Client 40 (XA)

Step 3: Enter database specific properties for the data source

Database name: OptimConsoleDB;create=true

When you are done, click **Save** to save the data source, and then click **Test connection** to test the data source.

2. Click **Applications > New Application > New Enterprise Application** and deploy the WAR file with the following properties. Use the defaults for all other properties:

Preparing for the application installation

The manager WAR file is *shared_installation_directory/console/app/optim.war*, where *shared_installation_directory* is the installation directory that you specified for the IBM

Optim Shared package group. For example, the default location for the manager WAR file on Microsoft Windows is C:\Program Files\IBM Optim\shared\console\app\optim.war. If you prefer, you can click **Browse** to browse for the file. Use **Fast Path** to install the application.

Step 3: Map resource references to resources

Click **Browse**, select **optimConsoleDS**, and click **Apply**.

Step 5: Map context roots for Web modules

Context Root: /optim

The WAR file can take several minutes to deploy. When you are done, click **Save** to save the configuration.

3. Click **Applications > Application types > WebSphere enterprise applications > optim_war > Security role to user/group mapping** and map the user roles available for the manager to the users or user groups in WebSphere Application Server. To map one or more roles to a set of users or user groups:
 - a. Select the box by each role that you want to map to users or user groups. You can map multiple roles to a user or user group.
 - b. Click **Map Users** to assign roles to users or **Map Groups** to assign roles to user groups.
 - c. Select the **Available** users or user groups that you want to map, click the right arrow button to move the users or user groups to **Selected**, and click **OK**.

When you are done, click **OK**, and click **Save**.

4. Click **Security > Global security**, select **Enable application security**, click **OK**, and click **Save**.
5. Click **Applications > Application types > WebSphere enterprise applications**, select the **Select** box for **optim_war** and click **Start**. The application can take several minutes to start.

You can now access the manager from a browser. The default location is `http://hostname:port/optim/console`. *hostname* is the name of the host on which you installed WebSphere Application Server, and *port* is the port number used by the manager. By default, the port number is 9080 when you deploy the manager on WebSphere Application Server.

Configuring the proxy

After you install the proxy and service execution components on the proxy computer, you must configure the proxy to run services.

Location of proxy product options file

Use the proxy product options file to set the proxy configuration properties. The proxy product options file is located at *proxy_folder/eclipse.ini*, where *proxy_folder* is the folder to which the proxy was installed. The default proxy folder depends on the operating system and on the user who installed the proxy.

- Default proxy folder on Microsoft Windows computers:
 - 32-bit: C:\Program Files\IBM Optim\proxy\
 - 64-bit: C:\Program Files (x86)\IBM Optim\proxy\
- Default proxy folder on Linux or UNIX computers:
 - Proxy installed by superuser: /opt/IBM/Optim/proxy/
 - Proxy installed by user other than superuser: /home/username/IBM/Optim/proxy/, where *username* is the name of the user who installed the proxy

Configuring the proxy to use the executor

If you want to use the proxy to run services with the executor, install the executor on the same computer as the proxy.

After you install the executor, open the *executor_folder/eclipse.ini* file and look for the following line, where *executor_folder* is the folder of the executor. If this line exists, set the line to the correct executor folder. You must always change this line if you install the executor on a computer with a 64-bit version of Windows. If this line does not exist, add the line to the file with the correct executor folder.

```
-Dcom.ibm.nex.executor.location=executor_folder
```

The default executor folder depends on the operating system and on the user who installed the executor.

- Default executor folder on Windows computers:
 - 32-bit: C:\Program Files\IBM Optim\executor
 - 64-bit: C:\Program Files (x86)\IBM Optim\executor
- Default executor folder on Linux or UNIX computers:
 - Executor installed by superuser: /opt/IBM/Optim/executor
 - Executor installed by user other than superuser: /home/username/IBM/Optim/executor, where *username* is the name of the user who installed the executor

Configuring the proxy to use the Optim pr0cmnd program

You can use the proxy to run services with the Optim pr0cmnd program as your service execution component. You must first install and configure Optim on the same computer as the proxy so that the pr0cmnd program is on the proxy computer. You must also install on the proxy computer the database client libraries for any relational database management systems that the services use. The proxy computer must be able to access a database that can be used to store the Optim Directory. Use Optim to run at least one service by itself to verify that the pr0cmnd program is configured properly and ready to run services.

When you run a service that uses the pr0cmnd command, the proxy uses the version of pr0cmnd in the following folder by default:

- Default program folder on Windows computers:
 - 32-bit: C:\Program Files\IBM Optim\RT\BIN
 - 64-bit: C:\Program Files (x86)\IBM Optim\RT\BIN
- Default program folder on Linux or UNIX computers: /opt/IBM/Optim/rt/bin

If the pr0cmnd program is in a folder other than the default folder, add the following argument to the end of the *proxy_folder/eclipse.ini* file. You must always add this argument if you install Optim on a computer with a 64-bit version of Windows.

```
-Dcom.ibm.nex.pr0cmnd.location=pr0cmnd_folder
```

- *pr0cmnd_folder* is the program folder for the pr0cmnd program.

For example, the following line specifies /opt/IBM/Optim/dist/bin as the name of the program folder for the pr0cmnd program.

```
-Dcom.ibm.nex.pr0cmnd.location=/opt/IBM/Optim/dist/bin
```

Configuring the proxy to send services to Optim for z/OS®

If you can successfully run an Optim for z/OS service from the designer, you can run the same service without any further configuration of the proxy. However, you might need to configure your network, firewalls, and IBM z/OS computer so that the proxy can successfully send the service to the z/OS computer.

Setting the registry and repository locations

By default, the proxy is set to use the registry and repository at `http://localhost:8080/server/registry` and `http://localhost:8080/server/repository`. These locations are valid if the registry and repository are on a management server that is installed on the proxy computer and that uses port 8080. By default, WebSphere Application Server Community Edition uses port 8080 for the management server. If the proxy and the registry and repository are on different computers, you must set the registry and repository locations for the proxy. You must also set registry and repository locations if you deploy the management server to an application server other than WebSphere Application Server Community Edition.

Open the `proxy_folder/eclipse.ini` file and look for the following lines, where `registry_URL` is the location of the registry and `repository_URL` is the location of the repository. If these lines exist, set the lines to the correct registry and repository locations. If these lines do not exist, add the lines to the file with the correct registry and repository locations.

```
-Dcom.ibm.optim.registry.url=registry_URL
-Dcom.ibm.optim.repository.url=repository_URL
```

For example, the following lines specify `http://mgmtserver1:8080/server/registry` as the registry location and `http://mgmtserver1:8080/server/repository` as the repository location.

```
-Dcom.ibm.optim.registry.url=http://mgmtserver1:8080/server/registry
-Dcom.ibm.optim.repository.url=http://mgmtserver1:8080/server/repository
```

Setting the host name and port for a proxy

If the proxy computer is assigned IP addresses dynamically, set the host name and port that are to be used by the proxy. To set the host name and port for the proxy, add the following arguments to the end of the `proxy_folder/eclipse.ini` file.

```
-Dcom.ibm.optim.host.name=host_name
-Dcom.ibm.optim.host.port=host_port
```

- `host_name` is the host name or IP address of the proxy.
- `host_port` is the port used by the proxy.

For example, the following lines specify `proxy_computer` as the host name of the proxy and 12000 as the port number used by the proxy.

```
-Dcom.ibm.optim.host.name=proxy_computer
-Dcom.ibm.optim.host.port=12000
```

Setting the shared library environment variable

When you install the proxy on Linux or UNIX, set the shared library environment variable to include the directory that contains the proxy libraries (`proxy_folder/shared/bin`). Set the shared environment variable for each account that is used to run the proxy. To set the shared library environment variable for an account, add the following lines to the account login profile.

- AIX:

```
LIBPATH=$LIBPATH:proxy_folder/shared/bin
export LIBPATH
```
- Linux or Solaris:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:proxy_folder/shared/bin
export LD_LIBRARY_PATH
```

Setting the proxy to use the https protocol

You can establish a trust relationship between a management server and a proxy. Among other things, you must set the proxy to use the https protocol to communicate with other components. The proxy uses

the http protocol unless you set the proxy to use the https protocol. To set the proxy to use the https protocol, add the following argument to the end of the *proxy_folder/eclipse.ini* file.

```
-Dcom.ibm.optim.url.protocol=https
```

For example, the following lines specify `https://mgmtserver1:8080/server/registry` as the registry location and `https://mgmtserver1:8080/server/repository` as the repository location.

```
-Dcom.ibm.optim.registry.url=https://mgmtserver1:8080/server/registry
-Dcom.ibm.optim.repository.url=https://mgmtserver1:8080/server/repository
-Dcom.ibm.optim.url.protocol=https
```

Configuring native data store (NDS) capabilities on a proxy

To configure a proxy to run services that use native data stores, install the relational database client software on the proxy computer. Then, use a native data store location property to specify the location of the native shared libraries that are installed with the database client. Add the native data store location property for the relational database system to the end of the *proxy_folder/eclipse.ini* file.

The following list contains the name of the native data store location property for each supported relational database system.

- DB2[®] for Linux, UNIX, and Windows: `com.ibm.nex.nds.rdbms.udb.location`
- DB2 for z/OS: `com.ibm.nex.nds.rdbms.db2.location`
- Oracle: `com.ibm.nex.nds.rdbms.oracle.location`
- Informix[®]: `com.ibm.nex.nds.rdbms.informix.location`

For example, the proxy is installed on a Linux computer, and the native shared libraries for DB2 for Linux, UNIX, and Windows are installed at `/opt/IBM/db2/V9.7/sql1lib/lib32`. To configure the NDS capability for DB2 for Linux, UNIX, and Windows on the proxy, add the following line to the end of the *proxy_folder/eclipse.ini* file.

```
-Dcom.ibm.nex.nds.rdbms.udb.location=/opt/IBM/db2/V9.7/sql1lib/lib32
```

Configuring the proxy to use the exact driver version specified on all service requests

By default, the proxy uses the JDBC driver that is specified on the service request or any newer version of the same driver. The proxy uses the first such driver that it finds in the repository. You can configure the proxy so that the proxy uses only the version of the JDBC driver that is specified on the service request. If the repository does not contain the version that is specified on the service request, the proxy returns an error. To configure the proxy so that the proxy uses only the exact driver version that is specified, add the following line to the end of the *proxy_folder/eclipse.ini* file:

```
-Dcom.ibm.nex.capability.driver.compatibility.level=enforceExactVersionMatch
```

Configuring the proxy to use UTF-8 encoding in logs

If you install the proxy on a computer that is set to a language that requires the use of double-byte characters, configure the proxy to use UTF-8 encoding in its log files. To configure the proxy to use UTF-8 encoding, add the following line to the end of the *proxy_folder/eclipse.ini* file.

```
-Dfile.encoding=UTF-8
```

On Windows computers, you must also add the following line, where *encoding* is the character encoding that is used by the Windows computer. For example, use MS932 for Shift JIS encoding.

```
-Dconsole.encoding=encoding
```

Setting file permissions

If you install the executor on a Linux or UNIX computer as a user other than the superuser, file permissions on your home directory might restrict users from using the executor. To correct this issue, complete either of the following tasks.

- Ask the administrator to install the executor to `/opt/IBM/Optim/executor`.
- Set the file permissions to the folder to which the executor is installed so that users can run the executor.

Configuring the proxy as a Windows service

If you install the proxy to a Microsoft Windows computer, you can configure the proxy to run as a Windows service. You can set the proxy service to restart automatically whenever the computer is restarted.

The proxy computer must have Microsoft .NET Framework 2.0 or higher installed.

To configure the proxy as a Windows service:

1. If the proxy is not installed to the default location at `C:\Program Files\IBM Optim\proxy`, complete the following steps:
 - a. Open the folder in which you installed the proxy.
 - b. Open the `proxyService.xml` file in that folder by using a text editor such as Notepad.
 - c. Change the value of the `proxyLocation` entity to the folder in which you installed the proxy.

For example, if you install the proxy to `D:\Applications\IBM Optim\proxy`, use Notepad to open `D:\Applications\IBM Optim\proxy\proxyService.xml` and change the `proxyLocation` value to `D:\Applications\IBM Optim\proxy`. On computers that run a 64-bit version of Windows, the proxy is installed to `C:\Program Files (x86)\IBM Optim\proxy` by default. You must therefore always edit the `proxyService.xml` file on computers that run a 64-bit version of Windows.

2. Open the command prompt by clicking **Start > Run** and entering the command `cmd`.
3. Enter the following commands at the command prompt, where *proxy_folder* is the folder in which the proxy is installed:

```
cd proxy_folder
proxyService.exe install
proxyService.exe start
```

You can check on the progress of the proxy by looking at the contents of log files. There are 3 log files:

- `proxy_folder/log/proxyService.err.log`
- `proxy_folder/log/proxyService.out.log`
- `proxy_folder/log/proxyService.wrapper.log`

To stop and uninstall the proxy service, enter the following commands at the command prompt.

```
cd proxy_folder
proxyService.exe stop
proxyService.exe uninstall
```

Configuring the proxy as a daemon on an AIX computer

If you install the proxy to a AIX computer, you can configure the proxy to run as a daemon process. You can set the proxy daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the proxy as a daemon on an AIX computer:

1. Open the command prompt.

2. Enter the following commands at the command prompt, where *proxy_folder* is the directory in which the proxy is installed:

```
cd proxy_folder
./setup-proxy-as-daemon.sh
```

The script generates a script called *optimproxy*, which is saved to the *proxy_folder* directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script *optimproxy* to the */etc/rc.d/init.d* directory.
5. Enter the following commands at the command prompt.

```
cd /etc/rc.d/init.d
chmod 755 optimproxy
ln -s optimproxy /etc/rc.d/rc2.d/S99optimproxy
ln -s optimproxy /etc/rc.d/rc2.d/K01optimproxy
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/rc.d/init.d/optimproxy start
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/rc.d/init.d/optimproxy stop
```

To remove the proxy daemon, log in as superuser and enter the following commands at the command prompt. Remove the proxy daemon before you uninstall the proxy.

```
/etc/rc.d/init.d/optimproxy stop
rm /etc/rc.d/rc2.d/S99optimproxy
rm /etc/rc.d/rc2.d/K01optimproxy
rm /etc/rc.d/init.d/optimproxy
```

Configuring the proxy as a daemon on a Linux computer

If you install the proxy to a Linux computer, you can configure the proxy to run as a daemon process. You can set the proxy daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the proxy as a daemon on a Linux computer:

1. Open the command prompt.
2. Enter the following commands at the command prompt, where *proxy_folder* is the directory in which the proxy is installed:

```
cd proxy_folder
./setup-proxy-as-daemon.sh
```

The script generates a script called *optimproxy*, which is saved to the *proxy_folder* directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script *optimproxy* to the */etc/rc.d/init.d* directory.
5. Enter the following commands at the command prompt.

```
cd /etc/rc.d/init.d
chmod 755 optimproxy
/sbin/chkconfig --add optimproxy
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/sbin/service optimproxy start
```

To view the init levels at which the daemon is started or stopped, log in as superuser and enter the following command at the command prompt.

```
/sbin/chkconfig --list optimproxy
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/sbin/service optimproxy stop
```

To remove the proxy daemon, log in as superuser and enter the following commands at the command prompt. Remove the proxy daemon before you uninstall the proxy.

```
/sbin/service optimproxy stop
/sbin/chkconfig --del optimproxy
rm /etc/rc.d/init.d/optimproxy
```

Configuring the proxy as a daemon on a Solaris computer

If you install the proxy to a Solaris computer, you can configure the proxy to run as a daemon process. You can set the proxy daemon to restart automatically whenever the computer is restarted.

You must have access to a superuser or root account to complete this task.

To configure the proxy as a daemon on a Solaris computer:

1. Open the command prompt.
2. Enter the following commands at the command prompt, where *proxy_folder* is the directory in which the proxy is installed:

```
cd proxy_folder
./setup-proxy-as-daemon.sh
```

The script generates a script called *optimproxy*, which is saved to the *proxy_folder* directory.

3. Log in as superuser, if you are not already logged in as superuser.
4. Copy the script *optimproxy* to the */etc/init.d* directory.
5. Enter the following commands at the command prompt.

```
cd /etc/init.d
chmod 755 optimproxy
ln -s optimproxy /etc/rc3.d/S99optimproxy
ln -s optimproxy /etc/rc3.d/K01optimproxy
```

To start the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/init.d/optimproxy start
```

To stop the daemon, log in as superuser and enter the following command at the command prompt.

```
/etc/init.d/optimproxy stop
```

To remove the proxy daemon, log in as superuser and enter the following commands at the command prompt. Remove the proxy daemon before you uninstall the proxy.

```
/etc/init.d/optimproxy stop
rm /etc/rc3.d/S99optimproxy
rm /etc/rc3.d/K01optimproxy
rm /etc/init.d/optimproxy
```

Configuring the executor

In most cases, you must configure features by configuring the component that launches the executor, rather than by configuring the executor itself. However, the location of the Social Security high-group file is configured in the executor product options file. The Social Security high-group file is used by services that validate or mask Social Security numbers.

Location of executor product options file

Use the executor product options file to set the executor configuration properties. The executor product options file is located at *executor_folder/eclipse.ini*, where *executor_folder* is the folder to which the executor was installed. The default executor folder depends on the operating system and on the user who installed the executor.

- Default executor folder on Microsoft Windows computers:
 - 32-bit: C:\Program Files\IBM Optim\executor\
 - 64-bit: C:\Program Files (x86)\IBM Optim\executor\
- Default executor folder on AIX, Linux, or Solaris computers:
 - Executor installed by superuser: /opt/IBM/Optim/executor/
 - Executor installed by user other than superuser: /home/username/IBM/Optim/executor/, where *username* is the name of the user who installed the executor

Location of the Social Security high-group file

By default, when the executor runs a service that validates or masks Social Security numbers, the executor uses the following high-group file:

<http://www.socialsecurity.gov/employer/highgroup.txt>

To change the location of the high-group file that is used by the executor, open the *executor_folder/eclipse.ini* file and find the line that specifies the `optim.datamask.ssn.highgroup.uri` property. Change the location at the end of the line to the location of the high-group file that you want to use.

For example, you want to use the high-group file at C:\my file\highgroup.txt. Open the *executor_folder/eclipse.ini* file, find the line that specifies the `optim.datamask.ssn.highgroup.uri` property, and change the line so that it matches the following line.

```
-Doptim.datamask.ssn.highgroup.uri=file:///C:\my file\highgroup.txt
```

Configuring the executor to use UTF-8 encoding in logs

If the executor computer is set to use a language that uses double-byte characters, configure the executor to use UTF-8 encoding in its log files. To configure the executor to use UTF-8 encoding, add the following line to the end of the *executor_folder/eclipse.ini* file.

```
-Dfile.encoding=UTF-8
```

Configuring the executor to log SQL warnings

You can configure the executor to log SQL warnings (that is, SQL messages whose error code is not equal to zero). SQL warnings are displayed in the proxy console when a service is run and are saved to the proxy log. To log SQL warnings, add the following line to the end of the *executor_folder/eclipse.ini* file.

```
-Dcom.ibm.optim.show.sql.warnings=true
```

Adding a trust relationship between a management server and a proxy

Add a trust relationship between a management server and a proxy to establish a Secure Sockets Layer (SSL) connection. Management servers and proxies can communicate securely only if you establish an SSL connection between these components.

This task must be performed only if the management server and proxy are on different computers and if the global preferences in the manager are set to require an SSL connection between the management server and proxy.

This task is performed by the administrators of the computers on which the management server and proxy are deployed.

Before you add a trust relationship between a management server and a proxy:

- Verify that you can access the keystore of the application server on which the management server is installed.
- Verify that you have command line access to the computer on which you have installed the proxy.

To add a trust relationship between a management server and a proxy:

1. Generate a certificate file for the application server on which the management server is installed. Ensure that the host name used in the certificate file is the exact host name that the proxy is to use to access the management server. You can use a public Certification Authority (CA) to generate a trusted certificate for the application server, or you can use the application server to set up a Certification Authority, self-generate a certificate, and save the certificate text to a text file. For information on how to use the application server to self-generate a certificate, see the security documentation for your application server.
2. If the management server and the proxy are on different computers, ensure that the proxy computer can access the certificate file from the management server computer. If necessary, copy the certificate file to the proxy computer.
3. Use the Java `keytool` key and certificate management utility with the `-importcert` option to import the certificate from the certificate file into the keystore of the proxy. The keystore location for each proxy is at `proxy_folder\jdk\jre\lib\security`, where `proxy_folder` is the folder in which the proxy is installed. For information on the `keytool` utility, see the Java documentation for the `keytool` utility.
4. Use the Java `keytool` key and certificate management utility with the `-genkeypair` option to generate a certificate file for the proxy. Ensure that the host name used in the certificate file is the exact host name that the management server is to use to access the proxy.
5. If the proxy and the application server are on different computers, ensure that the management server computer can access the certificate file from the proxy computer. If necessary, copy the certificate file to the management server computer.
6. Import the certificate from the certificate file into the keystore of the application server on which the management server is installed. For information on how to import a certificate into the application server, see the security documentation for your application server.

When you are done, you must configure both the management server and the proxy to use the https protocol to connect with other components.

Related reference

“Configuring the management server on WebSphere Application Server Community Edition” on page 11
After you deploy the management server to WebSphere Application Server Community Edition, you can configure management server properties. To configure management server properties, edit the script that you use to start WebSphere Application Server Community Edition.

“Configuring the proxy” on page 23

After you install the proxy and service execution components on the proxy computer, you must configure the proxy to run services.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator
Director of Engineering, Information Management (Office 16)
111 Campus Drive
Princeton, NJ 08540
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Index

A

account
 adding for the manager on WebSphere
 Application Server Community
 Edition 19

E

executor
 definition 2
 interactions with other components 3

M

management server
 configuring on WebSphere Application
 Server 20
 definition 1
 deploying WAR file on WebSphere
 Application Server 20
 deploying WAR file on WebSphere
 Application Server Community
 Edition 10
 interactions with other components 3
manager
 adding a user account on WebSphere
 Application Server Community
 Edition 19
 configuring on WebSphere Application
 Server 20
 definition 1
 deploying WAR file on WebSphere
 Application Server 22
 deploying WAR file on WebSphere
 Application Server Community
 Edition 17
 interactions with other components 3
 security 7
 user roles 7

O

Optim components
 configuring on WebSphere Application
 Server Community Edition 9
Optim Executor
 definition 2
Optim Management Server
 definition 1
Optim Manager
 adding a user account on WebSphere
 Application Server Community
 Edition 19
 definition 1
 deploying WAR file on WebSphere
 Application Server Community
 Edition 17
 interactions with other components 3

Optim Proxy
 definition 2

P

proxy
 definition 2
 interactions with other components 3
publisher
 definition 3

R

registry
 definition 1
repository
 definition 1
roles 7
 and system configuration 5
 and tasks 7
 assigning multiple to single user 7
 user roles
 and system setup 5

S

security 7
 user roles 7
service publisher
 definition 3
setup 5
SSL connection
 creating between components 30
system setup 5

T

trust relationship
 adding 30

U

user account
 adding for the manager on WebSphere
 Application Server Community
 Edition 19
user roles 7
 and tasks 7
 assigning multiple to single user 7

W

WAR file
 deploying management server on
 WebSphere Application Server 20
 deploying management server on
 WebSphere Application Server
 Community Edition 10

WAR file (*continued*)

 deploying manager on WebSphere
 Application Server 22
 deploying manager on WebSphere
 Application Server Community
 Edition 17
WebSphere Application Server
 configuring 20
 deploying management server WAR
 file on 20
 deploying manager WAR file on 22
WebSphere Application Server
Community Edition
 adding a user account for the
 manager 19
 configuring 9
 deploying management server WAR
 file on 10
 deploying manager WAR file on 17



Printed in USA