Oracle® Identity Manager

Installation and Configuration Guide for IBM WebSphere Application Server

Release 9.1.0.1

E14064-02

February 2009

ORACLE®

Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server
Release 9.1.0.1

E14064-02

Primary Author: Debapriya Datta

Contributing Author: Lyju Vadassery

Contents

4 Installing and Configuring a Database for Oracle Identity Manager

5 Installing Oracle Identity Manager on Microsoft Windows

6 Installing Oracle Identity Manager on UNIX or Linux

7 Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server

Preface

This guide explains the procedure to install Oracle Identity Manager release 9.1.0.1 on IBM WebSphere Application Server.

Audience

This guide is intended for system administrators of Oracle Identity Manager.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at http://www.consumer.att.com/relay/tty/standard2.html. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager release documentation set, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen (or text that you enter), and names of files, directories, attributes, and parameters.
`*_HOME`	This convention represents the directory where an application is installed. The directory where you install Oracle Identity Manager is referred to as *`OIM_HOME`*. Each Oracle Identity Manager component includes an abbreviation: *`OIM_DC_HOME`* for the Design Console and *`OIM_RM_HOME`* for the Remote Manager. The directory where the WebSphere application server is installed is referred to as *`WEBSPHERE_HOME`* and includes the `/WebSphere/AppServer/` directories. The directory where the WebSphere Client is installed is referred to as *`WEBSPHERE_CLIENT_HOME`* and includes the `/WebSphere/AppClient/` directories.

<Entry 1>.<Entry 2>.<Entry 3>	This convention represents nested XML entries that appear in files as follows:
	
	`<Entry 1>`
	`  <Entry 2>`
	`  <Entry 3>`

1

Overview of the Installation Procedure

Installing Oracle Identity Manager on IBM WebSphere Application Server involves:

1. Preparing for the installation: See Chapter 2, "Planning the Installation".
2. Setting up WebSphere for Oracle Identity Manager: See Chapter 3, "Installing and Configuring Nonclustered IBM WebSphere Application Server for Oracle Identity Manager".
3. Setting up a database for Oracle Identity Manager: See Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager".
4. Installing a single Oracle Identity Manager instance: See one of the following chapters based on the operating system:
   - Chapter 5, "Installing Oracle Identity Manager on Microsoft Windows"
   - Chapter 6, "Installing Oracle Identity Manager on UNIX or Linux"
5. Performing the basic Oracle Identity Manager and WebSphere configuration tasks related to the installation setup: See Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server".
6. Start Oracle Identity Manager and accessing the Administrative and User Console: See Chapter 8, "Starting and Stopping Oracle Identity Manager".
7. Deploy Oracle Identity Manager in a WebSphere cluster: See Chapter 9, "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration".
8. Installing, configuring, and starting the Oracle Identity Manager Design Console: See Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console".
9. Installing, configuring, and starting the Oracle Identity Manager Remote Manager: See Chapter 11, "Installing and Configuring the Oracle Identity Manager Remote Manager".
10. Troubleshooting the Oracle Identity Manager installation: See Chapter 12, "Troubleshooting the Oracle Identity Manager Installation".

2

Planning the Installation

Oracle recommends that you familiarize yourself with the components required for deployment before installing Oracle Identity Manager. Oracle also recommends that you install and use the Diagnostic Dashboard to ensure that your system is ready for Oracle Identity Manager installation. Refer to the "Using the Diagnostic Dashboard" section on page 2-5 for details of installing the Diagnostic Dashboard.

The basic Oracle Identity Manager installation consists of the following:

- Database server
- Application server
- Oracle Identity Manager running on the application server
- Design Console
- Administrative and User Console running on a Web browser

This chapter discusses the following topics:

2.1 Host Requirements for Oracle Identity Manager Components

This section lists the minimum host system requirements for the various components in an Oracle Identity Manager environment.

> **Note:** See *Oracle Identity Manager Readme* for the requirements and supported configurations specific to each version of the Oracle Identity Manager product.

You must obtain the enterprise versions of the application server and database software, complete with valid licenses. Oracle Identity Manager does not include this software.

The Oracle Identity Manager installation program can conflict with other installed applications, utilities, or drivers. Try to remove all nonessential software and drivers from the computer before installing Oracle Identity Manager. This practice also ensures that the database schema can be created in the database host.

2.1.1 Oracle Identity Manager Server (Host) Requirements

Table 2–1 lists the minimum host requirements for Oracle Identity Manager and the guidelines for a basic deployment.

Table 2–1 Oracle Identity Manager Server Requirements

Server Platform	Item	Requirement
Microsoft Windows and Linux	Processor Type	Intel Xeon or Pentium IV
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager instance
	Hard Disk Space	1 GB (initial size)
Solaris	Server	Sun Fire V210
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager instance
	Hard Disk Space	1 GB (initial size)
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager instance
	Hard Disk Space	1 GB (initial size)

2.1.2 Database Server Host Requirements

Table 2–2 provides sample database minimum host requirements for selective supported operating systems and must be considered only as guidelines. Consult the SQL Server or Oracle database documentation for the specific database host requirements.

Table 2–2 Sample Database Server Requirements

Database Server Platform	Item	Requirement
Microsoft Windows and Linux	Processor Type	Intel Xeon
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	2
	Memory	4 GB total or 2 GB for each CPU
	Hard Disk Space	40 GB (initial size)
Solaris	Server	Sun Fire V250
	Number of Processors	2
	Memory	4 GB total or 2 GB for each CPU

Table 2–2 (Cont.) Sample Database Server Requirements

Database Server Platform	Item	Requirement
	Hard Disk Space	40 GB (initial size)
	Number of Hard Disks	1 Disk
AIX	Processor Type	PowerPC
	Number of Processors	2
	Memory	4 GB total or 2 GB for each CPU
	Hard Disk Space	40 GB (initial size)

2.1.3 Design Console Host Requirements

Table 2–3 lists the minimum host requirements for the Oracle Identity Manager Design Console:

Table 2–3 Design Console Host Requirements

Design Console Platform	Item	Requirements
Microsoft Windows	Processor Type	Intel Pentium IV
	Processor Speed	1.4 GHz or higher
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	300 MB

2.1.4 Remote Manager Host Requirements

Table 2–4 lists the minimum host requirements for the Oracle Identity Manager Remote Manager:

Table 2–4 Remote Manager Host Requirements

Remote Manager Platform	Item	Requirement
Microsoft Windows and Linux	Processor Type	Intel Pentium IV
	Processor Speed	1.4 GHz or higher
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	1 GB
Solaris	Server	Sun Fire V210
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager instance
	Hard Disk Space	20 GB (initial size)
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory	512 MB

Table 2–4 (Cont.) Remote Manager Host Requirements

Remote Manager Platform	Item	Requirement
	Hard Disk Space	1 GB

2.2 Planning for Non-English Oracle Identity Manager Environments

If you are deploying Oracle Identity Manager Release components in non-English environments, then review the following guidelines and requirements:

- Before installing any of the Oracle Identity Manager Release components, ensure that the regional and language settings (locale) on the target system meet the following requirements:
  - An appropriate language version of the operating system is installed.
  - Specific language settings are properly configured.
- Refer to the *Oracle Identity Manager Globalization Guide* for information about configuring localized deployments and to ensure that you meet the character restrictions for various components and attributes.
- For Oracle database globalization support, you must configure the database for Unicode. Refer to "Creating an Oracle Database" on page 4-1 for more information.

2.3 Installation Worksheet

Table 2–5 provides information about the configuration attributes that you need before starting the Oracle Identity Manager installation. Print this worksheet and use it to take notes during the installation. Enter information specific to your installation in the User Selection column.

Table 2–5 Installation Worksheet

Item	Default	User Selection
The base directory for installing Oracle Identity Manager.	Microsoft Windows: `C:\oracle` UNIX or Linux: `/opt/oracle`	
The name or IP address of the computer on which the Oracle Identity Manager database is installed.	No default value	
The TCP port number on which the database listens for connections.	1521 for Oracle 1433 for Microsoft SQL Server	
The name of the database for your installation.	No default value	
The name and password of the database account that Oracle Identity Manager uses to access the database.	No default value	

Table 2–5 (Cont.) Installation Worksheet

Item	Default	User Selection
The JDK installation directory	Microsoft Windows: `C:\Program Files\IBM\WebSphere\AppServer\java` UNIX or Linux: `/opt/IBM/WebSphere/AppServer/java`	
The IBM WebSphere Application Server installation directory, known as *WEBSPHERE_HOME* throughout this document.	Microsoft Windows: `C:\Program Files\IBM\WebSphere\AppServer` UNIX or Linux: `/opt/IBM/WebSphere/AppServer`	

*NA = Not applicable for a default. However, you must enter a value for this item when you install Oracle Identity Manager.

2.4 Using the Diagnostic Dashboard

The Diagnostic Dashboard is a Web application that runs on the application server. It checks your preinstallation and postinstallation environments for components required by Oracle Identity Manager. Oracle recommends that you install the Diagnostic Dashboard before installing Oracle Identity Manager.

2.4.1 Installing the Diagnostic Dashboard

The Diagnostic Dashboard tool is distributed with the Oracle Identity Manager Installer CD media. It is located in the Diagnostic Dashboard directory.

You must deploy the Diagnostic Dashboard Web application on your application server.

> **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for more information about the Diagnostic Dashboard

2.4.2 Verifying Your Preinstallation Environment

You can use the Diagnostic Dashboard to verify that the components required to install Oracle Identity Manager are present:

- A supported Java Virtual Machine (JVM)
- A supported database
- Microsoft SQL Server JDBC libraries (only if you use Microsoft SQL Server)

> **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for information about the Diagnostic Dashboard

3

Installing and Configuring Nonclustered IBM WebSphere Application Server for Oracle Identity Manager

This chapter explains how to set up nonclustered IBM WebSphere Application Server before and after installing Oracle Identity Manager.

> **Note:** Refer to the "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" section on page 9-1 if you are using WebSphere in an application server cluster.

This chapter discusses the following topics:

- Overview of WebSphere Installation and Configuration
- Installing the WebSphere Application Server
- Installing the WebSphere Application Client
- Enabling SOAP Communication with WebSphere
- Obtaining the Bootstrap Port
- Upgrading the WebSphere Server and Client
- Setting Environment Variables
- Setting JVM Memory and Arguments
- Obtaining the WebSphere Cell and Node Name
- Preparing to Install Oracle Identity Manager as a Non-Root User on UNIX or Linux
- Starting WebSphere Before Installing Oracle Identity Manager

3.1 Overview of WebSphere Installation and Configuration

The following are high-level preinstallation and postinstallation tasks. You must perform all of these tasks.

1. Install the WebSphere Application Server: Refer to the "Installing the WebSphere Application Server" section on page 3-2.
2. Install WebSphere Application Client: Refer to the "Installing the WebSphere Application Client" section on page 3-2.

3. Enable SOAP Communication to WebSphere: Refer to the "Enabling SOAP Communication with WebSphere" section on page 3-2.
4. Upgrade WebSphere server and client software: Refer to the "Upgrading the WebSphere Server and Client" section on page 3-3.
5. Prepare the environment: Refer to the "Setting Environment Variables" section on page 3-4.
6. Increase the memory setting for the Java Virtual Machine: Refer to the "Setting JVM Memory and Arguments" section on page 3-4.
7. Obtain the cell and node name of the WebSphere instance on which you plan to install Oracle Identity Manager: Refer to the "Obtaining the WebSphere Cell and Node Name" section on page 3-5.
8. Install Oracle Identity Manager: Refer to the "Starting WebSphere Before Installing Oracle Identity Manager" section on page 3-6.

3.2 Installing the WebSphere Application Server

Install the appropriate WebSphere Application Server release supported by Oracle Identity Manager for a standalone and single server configuration.

Important: When installing the WebSphere Application Server, you must clear the **Enable administrative security** option on the Enable Administrative Security page of the WebSphere installer. By default, the **Enable administrative security** option is selected.

By default, this WebSphere Application Server installation creates the application server named `server1` under the profile named `AppSrv01`. Node is created with a naming convention of *`hostname`*`Node01`. Cell is created with a naming convention of *`nodename`*`Cell`. For example, if the host name is `oimtest`, then the node name is `oimtestNode01` and the cell name is `oimtestNode01Cell`.

Note: For a clustered configuration, you must use WebSphere Application Server Network Deployment.

3.3 Installing the WebSphere Application Client

The WebSphere Application Client is required to run the Oracle Identity Manager Design Console. Install the release of WebSphere Application Client (base) supported by Oracle Identity Manager. Refer to the WebSphere documentation for detailed installation procedures.

3.4 Enabling SOAP Communication with WebSphere

The Oracle Identity Manager Installer communicates with WebSphere as a SOAP client by using JACL commands to create data sources, set up message queues, and perform other operations.

To enable SOAP communication with WebSphere:

1. In a text editor, open the following file:

   `WEBSPHERE_HOME``/profiles/`*`PROFILE_NAME`*`/properties/soap.client.props`

Edit the property lines as follows:

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserid=xelsysadm
com.ibm.SOAP.loginPassword=xelsysadm_password
```

Note: If you have used a user ID or password other than `xelsysadm` when installing Oracle Identity Manager, then enter the same user ID and password here.

2. If you want to encode the password in the `soap.client.props` file, then run the `PropFilePasswordEncoder` command from the *WEBSPHERE_HOME*`/profiles/`*PROFILE_NAME*`/bin` directory.

   This command is specific to IBM WebSphere Application Server, and it encodes passwords located in plain-text property files. Refer to IBM WebSphere Application Server documentation for more details.

3. Save and close the file.

3.5 Obtaining the Bootstrap Port

During WebSphere Application Client installation, you are prompted for the WebSphere Server host name and port. The port is the WebSphere bootstrap port. You must also provide this port number during Design Console installation. Obtain the bootstrap port number by using the WebSphere administrative console.

Note: The WebSphere application server must be running to obtain the bootstrap port number.

To view the bootstrap port number on a nonclustered installation:

1. Log on to the WebSphere administrative console.
2. Select **Servers, Application Servers**, <SERVER_NAME>, and then select **Ports** under Communication.

   The bootstrap port is displayed as BOOTSTRAP_ADDRESS.

To view the bootstrap port number on a clustered installation:

1. Log on to the WebSphere administrative console.
2. Select **System Administration**, **Deployment Manager,** then select **Ports** under Additional Properties.

   The bootstrap port is displayed as `BOOTSTRAP_ADDRESS`.

3.6 Upgrading the WebSphere Server and Client

Both the WebSphere Application Server and the Client must be updated with the Oracle Identity Manager fix packs from IBM.

Perform the following upgrades in the following sequence:

1. Upgrade the WebSphere Application Server.

2. Upgrade the JDK for WebSphere server.
3. Upgrade your WebSphere Client.
4. Upgrade the JDK for WebSphere Client.

> **Note:** See *Oracle Identity Manager Readme* for this release for information about the minimum certified versions of WebSphere fix packs and JDK fixes required by Oracle Identity Manager.
>
> Oracle Identity Manager supports all JDK fixes and WebSphere fix packs on top of the minimum certified versions.

3.7 Setting Environment Variables

The following environment variable settings are necessary for Oracle Identity Manager Installer:

- Ensure that the `JAVA_HOME` system variable is set to the appropriate JDK. On Microsoft Windows, Solaris, and Linux, set `JAVA_HOME` to Sun JDK. On AIX, set `JAVA_HOME` to the IBM JDK (bundled with IBM WebSphere).

  > **See Also:** *Oracle Identity Manager Readme* for information about certified JDK versions

- Remove the `ANT_HOME` system variable if it is defined.
- For Microsoft Windows, Solaris, and Linux, ensure that the Sun JDK is being used when a Java command is run. To do this, include the `/java/jre/bin/` directory of the Sun JDK installation in the `PATH` ahead of all other path entries. For example:

  Microsoft Windows:

  ```
  set PATH=SUN_JDK_HOME\jre\bin;%PATH%
  ```

  Solaris or Linux

  ```
  export PATH=SUN_JDK_HOME/jre/bin:$PATH
  ```

- For AIX, ensure that the IBM JDK (bundled with IBM WebSphere) is being used when a Java command is run. To do this, include the `/java/jre/bin/` directory of IBM JDK installation in the PATH ahead of all other path entries. For example:

  ```
  export PATH=IBM_JDK_HOME/jre/bin:$PATH
  ```

3.8 Setting JVM Memory and Arguments

For Oracle Identity Manager, JVM memory settings must be changed for production environments and/or when processing large volume in nonproduction.

Perform the following steps to set the JVM memory size. The WebSphere application server must be running to set the memory size.

To set the JVM memory size:

1. Connect to the WebSphere administrative console by using the following URL:

   ```
   http://WebSphere Host:WebSphere Admin Port/admin
   ```

Note: The default WebSphere administrative console port is 9060.

2. Select **Servers**, and then select **Application Servers**.
3. Select the server name.
4. Go to Server Infrastructure, and then click **Java and Process Management.**
5. Select **Process Definition**.
6. Go to Additional Properties, and then click **Java Virtual Machine.**
7. Enter **1280** for Minimum Heap Size.
8. Enter **1280** for Maximum Heap Size.
9. Enter `-Xjit:disableLocalVP,disableGlobalVP` for Generic JVM arguments.
10. Click **OK**.
11. Click **Save** to commit the setting.

Note: For clustered installation of WebSphere, these changes must be done for all the servers participating in the cluster.

3.9 Obtaining the WebSphere Cell and Node Name

After installing and initially configuring WebSphere, you must obtain the cell and node name of the WebSphere instance on which you plan to install Oracle Identity Manager. The Oracle Identity Manager Installer will prompt you for this information during the installation.

To obtain the cell and node name:

1. Connect to the WebSphere administrative console by using the following URL:

   `http://`*`WebSphere Host`*`:`*`WebSphere Admin Port`*`/admin`

2. In the left pane, click **Servers**.
3. Click **Application Servers** under **Servers**.
4. Click the **server instance** (server1, default) on the right section.
5. Click the **Runtime** tab.
6. Note the values for **Cell Name** and **Node Name**.

Note: If the value of State is not `Started`, then restart the server instance.

3.10 Preparing to Install Oracle Identity Manager as a Non-Root User on UNIX or Linux

Installing Oracle Identity Manager as a non-root user on a WebSphere application server running on UNIX or Linux requires certain permissions. Before attempting to install Oracle Identity Manager as a non-root user on a WebSphere application server running on UNIX or Linux, verify that the operating system user account installing

Oracle Identity Manager has write and execute permissions on the directories in which WebSphere will be installed.

3.11 Starting WebSphere Before Installing Oracle Identity Manager

The Oracle Identity Manager Installer communicates with the WebSphere server during installation. Therefore, you must verify that the application server is running before you start the installation.

To start WebSphere on Microsoft Windows, use the Windows **Start** menu, or the *WEBSPHERE_HOME*\profiles*PROFILE_NAME*\bin\startServer.bat script. For example, run:

```
WEBSPHERE_HOME\profiles\PROFILE_NAME\bin\startServer.bat server name
```

To start WebSphere on UNIX or Linux, use the *WEBSPHERE_HOME*/profiles/*PROFILE_NAME*/bin/startServer.sh script. For example, run:

```
WEBSPHERE_HOME/profiles/PROFILE_NAME/bin/startServer.sh server name
```

To install Oracle Identity Manager, follow the installation instructions in the chapter specific to your operating system. Refer to the "Installing Oracle Identity Manager on Microsoft Windows" section on page 5-1 or the "Installing Oracle Identity Manager on UNIX or Linux" section on page 6-1 for more information.

4

Installing and Configuring a Database for Oracle Identity Manager

Oracle Identity Manager requires a database. You must install and configure your database before you begin the Oracle Identity Manager installation. Refer to the topic that applies to your database:

- Using an Oracle Database for Oracle Identity Manager
- Using Oracle RAC Databases for Oracle Identity Manager
- Using a Microsoft SQL Server Database for Oracle Identity Manager

4.1 Using an Oracle Database for Oracle Identity Manager

The following are the high-level tasks for using an Oracle Database for Oracle Identity Manager.

1. Install Oracle. Refer to the "Installing Oracle Database" section on page 4-1.
2. Create an Oracle Database. Refer to the "Creating an Oracle Database" section on page 4-1.
3. Prepare the Database. Refer to the "Preparing the Oracle Database" section on page 4-2.

4.1.1 Installing Oracle Database

Install Oracle9*i* Database or Oracle Database 10*g* release 2 by referring to the documentation delivered with the Oracle database. See *Oracle Identity Manager Readme* for the specific supported versions. Oracle recommends using the Basic installation.

> **Note:** If you choose the Custom installation, then you must include the JVM option, which is required for XA transaction support.

4.1.2 Creating an Oracle Database

You can create a new Oracle database instance for Oracle Identity Manager. When creating the database, ensure that you configure the Oracle JVM feature and enable query rewrite.

You can use the Database Configuration Assistant (DBCA) tool to create the database. To configure the Oracle JVM feature, select the Oracle JVM feature on the Standard Database Features page of the DBCA.

To enable the database for query rewrite, set the initialization parameters `QUERY_REWRITE_ENABLED` to `TRUE` and `QUERY_REWRITE_INTEGRITY` to `TRUSTED` in the **All Initialization Parameters** field of the DBCA.

> **Note:** For the Oracle Identity Manager installation, Oracle recommends that you configure a minimum block size of 8K for Oracle Database.

Consult your Oracle Database documentation for detailed instructions on creating a database instance.

4.1.2.1 Configuring the Database for Globalization Support

For globalization support for Oracle Identity Manager Release, Oracle recommends that configuring the database for Unicode. To configure the database for Unicode, perform the following steps:

1. Select **AL32UTF8** in the Character Sets tab of the DBCA. This character set supports the Unicode standard.
2. Set the `NLS_LENGTH_SEMANTICS` initialization parameter to `CHAR` in the **All Initialization Parameters** field of the DBCA.

> **See Also:** *Oracle Identity Manager Globalization Guide* for more information about globalization support in Oracle Identity Manager

4.1.3 Preparing the Oracle Database

After you install Oracle Database and create a database instance, you must prepare it for Oracle Identity Manager by completing the following tasks:

- Verify that query rewrite is enabled

> **Note:** Query rewrite is applicable only if you are using Oracle Database Enterprise Edition.

- Enable XA transactions support

> **Note:** Java Virtual Machine (JVM) is required to enable XA transaction support. If you did not install the Oracle JVM component during Oracle Database installation, then you must install it now. See the Oracle Database documentation for specific instructions.

- Create at least one tablespace for storing Oracle Identity Manager data
- Create a database user account for Oracle Identity Manager

You can perform the preceding tasks to prepare the Oracle database for Oracle Identity Manager by running one of the following scripts:

- UNIX or Linux:

```
prepare_xl_db.sh
```

- Microsoft Windows:

```
prepare_xl_db.bat
```

Both of these scripts ship with the Oracle Identity Manager Installer and are in the `\installServer\Xellerate\db\oracle\` directory.

The prerequisites to run the prepare_xl_db scripts are:

- The script must be run by a user holding DBA privilege. For example, the oracle user on UNIX or Linux typically holds these privileges.
- The script must be run on the computer in which the database is installed.

To prepare your Oracle database for Oracle Identity Manager, complete the steps associated with the operating system on the computer hosting the Oracle database.

4.1.3.1 Preparing on UNIX or Linux

To prepare the scripts on UNIX or Linux:

1. Copy the prepare_xl_db.sh and xell_db_prepare.sql scripts from the distribution CD to a directory on the computer hosting the database in which you (as the account user performing this task) have write permission.
2. Run the following command to enable execute permission for the script:

   ```
   chmod 755 prepare_xl_db.sh
   ```

3. Run the script prepare_xl_db.sh by entering the following command:

   ```
   ./prepare_xl_db.sh
   ```

4. Provide information appropriate for the database and host computer when the script prompts you for the following items:
   - The location of your Oracle home, which is *ORACLE_HOME*
   - The name of the database, which is ORACLE_SID
   - The name of the Oracle Identity Manager database user to be created
   - The password for the Oracle Identity Manager database user
   - The name of the tablespace to be created for storing Oracle Identity Manager data
   - The directory to store the data file for the Oracle Identity Manager tablespace
   - The name of the data file (You do not append the .dbf extension.)
   - The name of the temporary tablespace
5. Check the prepare_xl_db.lst log file located in the directory in which you ran the prepare_xl_db script to see execution status and additional information.

Note: If you encounter errors after running the prepare_xl_db.sh script, then run the following command to ensure that the prepare_xl_db.sh is executable on UNIX and Linux, and then run the prepare_xl_db.sh script again.

```
$ dos2unix prepare_xl_db.sh
```

4.1.3.2 Preparing on Microsoft Windows

To prepare the scripts on Microsoft Windows:

1. Copy the prepare_xl_db.bat and xell_db_prepare.sql scripts from the distribution CD to a directory on the computer hosting the database in which you (as the account user performing this task) have write permission.
2. Open a command prompt, navigate to the directory in which you copied the scripts, and run prepare_xl_db.bat with the following arguments:

   ```
   prepare_xl_db.bat ORACLE_SID ORACLE_HOME XELL_USER XELL_USER_PWD
   TABLESPACE_NAME DATAFILE_DIRECTORY DATAFILE_NAME XELL_USER_TEMP_TABLESPACE
   SYS_USER_PASSWORD
   ```

   For example, the string you enter on the command line might look similar to the following:

   ```
   prepare_xl_db.bat XELL C:\oracle\ora92 xladm xladm xeltbs C:\oracle\oradata
   xeltbs_01 TEMP manager
   ```

   Table 4–1 lists the options used in the preceding example of prepare_xl_db.bat.

Table 4–1 Options for the prepare_xl_db.bat Script

Argument	Description
`XELL`	Name of the database
`C:\oracle\ora92`	Directory in which the Oracle database is installed
`xladm`	Name of the Oracle Identity Manager user to be created
`xladm`	Password for the Oracle Identity Manager user
`xeltbs`	Name of the tablespace to be created
`C:\oracle\oradata`	Directory in which the data files will be placed
`xeltbs_01`	Name of the data file (you do not need to include the .dbf extension)
`TEMP`	Name of the temporary tablespace that already exists in the database
`manager`	Password for the SYS user

3. Check the `prepare_xl_db.lst` log file located in the directory in which you ran the xell_db_prepare script to see execution status and additional information.

4.1.3.3 Interpreting the Script Results

If the script returns a message indicating successful execution, then you can continue to the next task, which is Oracle Identity Manager installation.

If the script does not succeed, then you must manually fix all fatal (nonrecoverable) errors so that the database is prepared successfully.

You can ignore all nonfatal errors. For example, when the script tries to drop a nonexistent view, it will return the error `"ORA-00942: table or view does not exist"`.

Ensure that you scan all the errors in the log file and ignore or resolve them on an individual basis. Remember that you must successfully prepare the database for Oracle Identity Manager before you can install Oracle Identity Manager.

4.1.4 Removing Oracle Identity Manager Entries from an Oracle Database

To remove Oracle Identity Manager entries from an Oracle database after removing Oracle Identity Manager, drop the database user holding the Oracle Identity Manager schema.

4.2 Using Oracle RAC Databases for Oracle Identity Manager

This section explains how to deploy Oracle Real Application Clusters (Oracle RAC) databases for Oracle Identity Manager. It discusses the following sections:

- Installing Oracle Identity Manager for Oracle RAC
- Oracle RAC Net Services
- JDBC and Oracle RAC
- Configuring IBM WebSphere Application Server for Oracle RAC

4.2.1 Installing Oracle Identity Manager for Oracle RAC

Oracle RAC is a cluster database with a shared cache architecture that provides highly scalable and available database solutions. Oracle RAC consists of multiple database instances on different computers. These database instances act in tandem to provide the database solutions.

Note: The Oracle Identity Manager Installer program does not provide support for Oracle RAC. To deploy Oracle Identity Manager for Oracle RAC, you must install Oracle Identity Manager on a single database instance in Oracle RAC and then change the application server settings, specifically the connection pool parameters, to use the Oracle RAC JDBC connection string.

Perform the following steps to install Oracle Identity Manager for Oracle RAC:

1. Ensure that Oracle RAC is properly set up and configured with the Oracle Identity Manager schema owner.
2. Start the Oracle Identity Manager Installer.
3. On the Database Parameters page of the installer, enter the host name, port number, and database name of a single database instance in Oracle RAC.
4. Complete the Oracle Identity Manager installation by performing the steps in the installer.
5. Configure your application server for Oracle RAC. Refer to the "Configuring IBM WebSphere Application Server for Oracle RAC" section on page 4-6.

4.2.2 Oracle RAC Net Services

The net services name entry for an Oracle RAC database differs from that of a conventional database. The following is an example of the net services name entry for an Oracle RAC database:

```
racdb=
        (DESCRIPTION=
                  (LOAD_BALANCE=off)
                  (FAILOVER=on)
                  (ADDRESS_LIST=
```

```
                    (ADDRESS=(protocol=tcp)(host=node1-vip)(port=1521))
                    (ADDRESS=(protocol=tcp)(host=node2-vip)(port=1521)))
  (CONNECT_DATA=
            (SERVER=DEDICATED)
            (SERVICE_NAME=racdb)))
```

Table 4–2 describes the parameters in a net services name entry for an Oracle RAC database.

Table 4–2 Parameters for Oracle RAC Database Net Services Name Entries

Parameter	Description
LOAD_BALANCE	Specifies whether client load balancing is enabled (on) or disabled (off). The default setting is on.
FAILOVER	Specifies whether failover is enabled (on) or disabled (off). The default setting is on.
ADDRESS_LIST	Specifies the list of all the nodes in Oracle RAC, including their host names and the ports they listen on.

4.2.3 JDBC and Oracle RAC

JDBC client applications that use the Thin driver to connect to an Oracle RAC database must use the Oracle RAC net services name as a part of the JDBC URL. The entire Oracle RAC net services name is concatenated, and the entire string is used in the JDBC URL so that the client application can connect to Oracle RAC.

The following sample code shows how a JDBC URL is used to connect to an Oracle RAC database:

```
//String url = "jdbc:oracle:thin:@dbhost:1521:dbservice"
String racUrl =
"jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_LIST=(ADDR
ESS=(protocol=tcp)(host=node1-vip)(port=1521))(ADDRESS=(protocol=tcp)(host=node2-v
ip)(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=racdb)))";

       String strUser = "username";
       String strPW = "password";

       // load Oracle driver
       Class.forName("oracle.jdbc.driver.OracleDriver");

       // create the connection
       con = DriverManager.getConnection(strURL, strUser, strPW);
```

The subsequent sections about configuring application servers for Oracle RAC databases explain how to modify connection pools to use a similar JDBC URL so that the application server can communicate with Oracle RAC.

4.2.4 Configuring IBM WebSphere Application Server for Oracle RAC

This section explains how to configure IBM WebSphere Application Server (nonclustered or clustered) for Oracle RAC by ensuring that the data sources and connection pools are configured to use the Oracle RAC JDBC connection string.

Note: Before configuring WebSphere application servers for Oracle RAC, you must:

- Get the RAC net services name from the tnsnames.ora file.
- Construct the RAC JDBC URL. Refer to the "JDBC and Oracle RAC" section on page 4-6.

Perform the following steps to configure both nonclustered and clustered WebSphere application servers for Oracle RAC:

1. Open the *OIM_HOME*/xellerate/config/xlconfig.xml file.
2. Locate the <DirectDB> section and replace the value of the <url>...</url> tag with the RAC JDBC URL. For example, the new tag might be similar to the following:

```
<url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_
LIST=(ADDRESS=(protocol=tcp)(host=node1-vip)(port=1521))(ADDRESS=(protocol=tcp)
(host=node2-vip)(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_
NAME=racdb)))</url>
```

3. Save and close the *OIM_HOME*/xellerate/config/xlconfig.xml file.
4. Log on to the WebSphere Administrative Console by using a Web browser if you are configuring a nonclustered WebSphere environment. Log on to the WebSphere Administrative Console of the Network Deployment Manager (NDM) by using a Web browser if you are configuring a clustered WebSphere environment.
5. Select **Resources**, **JDBC**, **Data Sources**, and then select **Non XA DataSource.**

   At the bottom of the page, replace/set the value of URL property to RAC JDBC URL as described in step 2.
6. Save the settings.
7. Select **Resources**, **JDBC**, Data Sources, and then select **XADataSource.**

   At the bottom of the page, replace/set the value of URL property to RAC JDBC URL as described in step 2.
8. Save the settings.
9. Restart the WebSphere application server if you are configuring a nonclustered WebSphere environment. Restart the WebSphere NDM if you are configuring a clustered WebSphere environment.

4.3 Using a Microsoft SQL Server Database for Oracle Identity Manager

To use Microsoft SQL Server as the database, perform the procedures described in the following sections:

- Installing and Configuring Microsoft SQL Server
- Creating a Microsoft SQL Server 2005 Database
- Creating a Microsoft SQL Server Database Account
- Removing Oracle Identity Manager Entries from a Microsoft SQL Server Database

4.3.1 Installing and Configuring Microsoft SQL Server

To install and configure Microsoft SQL Server 2005 for Oracle Identity Manager:

1. Install Microsoft SQL Server 2005 with Service Pack 2.

   During installation, select **mixed authentication mode**, and then set the password to that of the sa user.

   > **Note:** Perform Steps 2 through 4 on the computer hosting the application server.

2. Download the SQL Server 2005 Driver for JDBC from the Microsoft Web site.
3. Install SQL Server 2005 Driver for JDBC.

   Instructions to install JDBC drivers for SQL Server 2005 are available at the following location:

   SQL_SERVER_HOME\sqljdbc_1.2\enu\help\html\574e326f-0520-4003-bdf1-62d92c3db457.htm

   > **Note:** Specify a short path for the installation folder, such as C:\JDBCjars, so that you can easily add the path to your CLASSPATH in the next step. If the classpath is more than 256 characters, then the installer does not work properly.

4. Locate the JDBC driver file (sqljdbc.jar) from the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\ directory.

   Add their location to the system CLASSPATH environment variable. If the CLASSPATH environment variable does not exist, you must create it. The string you add should look like the following:

   C:*jdbc_install_folder*\sqljdbc.jar;

   In this sample string, *jdbc_install_folder* is the location where the SQL Server 2005 Driver for JDBC files is installed.

   > **Note:** Perform Steps 5 through 7 on the computer hosting the Microsoft SQL Server database.

5. On the computer hosting the Microsoft SQL Server database, enable distributed transactions by installing SQL Server 2005 JDBC XA procedures.

   Copy the sqljdbc.dll file from the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\xa\x86\ directory to the *Microsoft_SQL_Server_HOME*\MSSQL\Binn\ directory.

6. Run the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\xa\xa_install.sql script.
7. Ensure that the Distributed Transaction Coordinator (MSDTC) service for your SQL Server is running.

   If necessary, restart SQL Server 2005.

4.3.2 Creating a Microsoft SQL Server 2005 Database

The following procedure describes how to create a new database for Oracle Identity Manager.

> **Note:** From this point onward in the guide, the name XELL is used to refer to the database. You can set any name for the database.

To create a SQL Server database:

1. Start the Microsoft SQL Server Management Studio application as follows:
   a. From the Windows Start menu, expand **All Programs**, expand **Microsoft SQL Server 2005**, and then select **SQL Server Management Studio**.
   b. In the Connect to Server dialog box, verify the default settings. Ensure that the name of the computer on which SQL Server is installed is specified in the Server name box. Then, click **Connect**.
2. On the left pane of the SQL Server Management Studio application window, right-click **Databases**, and then select **New Database**.
3. In the New Database Properties dialog box, on the left pane, select **General**, and then enter **XELL** in the Database Name field.
4. In the Database Files section, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 4–3.

Table 4–3 Database Files

Logical Name	File Type	File Group	Initial Size in Megabytes (MB)	Auto Growth	Path	File Name
XELL_PRIMARY	Data	PRIMARY	100	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_DATA	Data	XELL_DATA	500	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_INDEX	Data	XELL_INDEX	300	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_TEXT	Data	XELL_TEXT	500	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_UPA	Data	XELL_UPA	1000	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)

Note:

- Table 4–3 lists initial sizes for a production environment. For non-production installations, you can use the default initial sizes provided for the filegroups.
- To ensure successful installation of Oracle Identity Manager, filegroup names must be entered exactly as they appear in Table 4–3. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.
- The PRIMARY filegroup contains the system objects required for SQL Server to operate. The XELL_DATA filegroup stores the physical data and primary keys, XELL_INDEX filegroup stores indexes, XELL_TEXT stores large text fields and XELL_UPA stores physical data and primary keys of the User Profile Audit component.

5. Select the log file, then change the initial size to 500 MB. Leave all the other options on the tab at their default values.

Note: For nonproduction installations, you can use the default initial size for the log file.

6. Click **OK** to start creating the database.

4.3.3 Creating a Microsoft SQL Server Database Account

The following procedure describes how to create a database account for Oracle Identity Manager and assign appropriate permissions to that account.

Note: The following procedure assumes the account name xladm. If you want to use an account name other than xladm, then specify that login instead of xladm throughout the following procedure and also when installing Oracle Identity Manager.

To create a Microsoft SQL Server database account and permissions:

1. Start the Microsoft SQL Server Management Studio application.
2. On the left pane of the SQL Server Management Studio application window, select **Security**, right-click **Logins**, and then select **New Login**.
3. In the SQL Server Login Properties dialog box, from the left pane, click the **General** tab, and perform the following steps:
   a. In the Login Name field, enter **xladm** (or a different account name that you prefer).
   b. Select the **Enforce Password Policy** check box. Deselect all other check boxes.
4. Select **SQL Server Authentication**, and then enter the password associated with the account you specified in the Password field.
5. In the **Database** box within the **Defaults** section, select **XELL** from the list.

Leave the **Language** box set to <default>.

6. Select the **User Mapping** option from the left pane.
7. In the upper panel, select the check box associated with **XELL**. Set the XELL in the Default Schema column.
8. In the lower panel, select the check boxes associated with the following:
   - public
   - db_owner
   - db_accessadmin
   - db_securityadmin
   - db_ddladmin
   - db_datareader
   - db_datawriter
9. Select the check box associated with master. Set the XELL in the Default Schema column.
10. In the lower panel, select the check boxes associated with the following:
    - public
    - SqlJDBCXAUser
11. Click **OK** to commit your changes.
12. On the Microsoft SQL Server Management Studio, in the left pane, right-click registered server, click Properties. In the Properties dialog box, select the Security option, and then verify that Authentication is set to SQL Server and Windows.
13. Start the Microsoft SQL Server 2005 Surface Area Configuration application. To do so:
    a. From the Start menu, expand **All Programs**, expand **Microsoft SQL Server 2005**, expand **Configuration Tools**, and then click **SQL Server 2005 Surface Area Configuration**. A dialog box is displayed.
    b. Click **Surface Area Configuration for Services and Connection**. On the left pane, select the **MSSQLSERVER-> Database Engine**, and then verify that the Startup Type is set to **Automatic**.
    c. If Autostart SQL Server Agent is selected, do not change the existing setting, because that setting may be required by other applications. Click **OK** to close the SQL Server Properties page.

4.3.4 Removing Oracle Identity Manager Entries from a Microsoft SQL Server Database

To remove Oracle Identity Manager entries from a Microsoft SQL Server 2005 database after removing (deinstalling) the Oracle Identity Manager product:

1. Delete the Oracle Identity Manager database.
2. Delete the Oracle Identity Manager login.

5

Installing Oracle Identity Manager on Microsoft Windows

This chapter explains how to install Oracle Identity Manager on Microsoft Windows in a nonclustered installation.

> **See Also:** Chapter 9, "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" for information about deploying Oracle Identity Manager in a clustered installation

You must install Oracle Identity Manager on systems running the application server. Oracle Identity Manager components such as the Remote Manager and Design Console can be installed on separate systems. Each component has its own installer.

This chapter discusses the following topics:

- Installing the Database Schema
- Installing Documentation
- Installing Oracle Identity Manager on Microsoft Windows
- Removing Oracle Identity Manager

> **Caution:** Do *not* use a remote client tool, such as Symantec pcAnywhere, to install Oracle Identity Manager products.

5.1 Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into the database. You only install the database schema once. It is installed the first time you run the Oracle Identity Manager Installer. Each time you run the installer to deploy other Oracle Identity Manager components, you enter information about the database connection to configure the component for the same schema. If required, contact your database administrator (DBA).

> **Note:** During the schema installation, a log file is created in the *OIM_HOME*\logs directory.

5.2 Installing Documentation

Oracle Identity Manager documentation is installed automatically in the *OIM_HOME* directory. A full documentation set is installed with each Oracle Identity Manager component.

5.3 Installing Oracle Identity Manager on Microsoft Windows

This section describes how to install Oracle Identity Manager on a computer running Microsoft Windows.

Caution: Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. For each new installation, use a different home directory. If you want to reuse the name of an existing Oracle Identity Manager home directory, then back up your original Oracle Identity Manager home by renaming that directory.

Remember that all Oracle Identity Manager components must be installed on different home directories. For example, you cannot install the Remote Manager in the same directory as Oracle Identity Manager.

To install Oracle Identity Manager on a Microsoft Windows host:

1. Before installing Oracle Identity Manager, you must set the *JAVA_HOME* and `PATH` variables by following the procedure specific to the operating system that you use. Refer to the "Setting Environment Variables" section on page 3-4 for information about setting environment variables.
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

   Note: If the autostart routine is enabled for the computer, then proceed to Step 3.

   ---

3. Using the Windows Explorer, navigate to the `installServer` directory on the installation CD, and double-click the **setup_server.exe** file.
4. Select a language on the Installer page and click **OK**. The Welcome page is displayed.
5. Click **Next** on the Welcome page. The Admin User Information page is displayed.
6. Enter the password that you want to use as the Oracle Identity Manager administrator, confirm the password by entering it again, and then click **Next**. The OIM Application Options page is displayed.
7. Select one of the following applications to install, and then click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module

     See Also: *Oracle Identity Manager Audit Report Developer's Guide* for information about the Audit and Compliance Module
8. After the Target directory page is displayed, complete one of the following:

- The default directory for Oracle Identity Manager is `C:\oracle`. To install Oracle Identity Manager into this directory, click **Next**.
- To install Oracle Identity Manager into another directory, enter the path in the Directory field, and then click **Next**.

Or:

Click **Browse**, navigate to the desired location, and then click **Next**.

Note: If the directory path does not exist, then the Base Directory settings field is displayed. Click **OK**. The directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message, and then contact your system administrator to obtain the appropriate permissions.

---

9. On the Database Server Selection page, specify the type of database that you are using with Oracle Identity Manager, then click **Next**.
10. On the Database Information page, provide all database connectivity information that is required to install the database schema.

    You install this schema just once, as part of your initial Oracle Identity Manager installation. After this, you configure all the other Oracle Identity Manager components to point to this common schema.

Note: To install against an existing database, verify that the release of Oracle Identity Manager you are installing is certified with the existing database version. See *Oracle Identity Manager Readme* for information about certified configurations.

When Oracle Identity Manager is installed against an existing database, a warning message is displayed indicating that the database schema already exists and instructing you to copy the .xldatabasekey file from the existing Oracle Identity Manager installation to the new *OIM_HOME*`\xellerate\config\` directory after you complete the installation process.

You must create the `\config` directory in the new *OIM_HOME*`\xellerate\` path if it does not exist.

- In the **host** field, enter the host name or the IP address of the computer on which the database is installed.
- In the **PORT** field, enter the port number on which the database listens for connections. The default port is 1521 for Oracle Database and 1433 for Microsoft SQL Server.
- In the **Database SID** field, enter the name of the database instance.
- In the **User Name** field, enter the user name of the database account that you created for Oracle Identity Manager.
- In the **Password** field, enter the Oracle Identity Manager database user password.
- Click **Next** to commit the settings.

Note: When you set the preceding items, see the configuration settings specified in "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a Microsoft SQL Server Database for Oracle Identity Manager" on page 4-7 to verify your settings.

The installer checks for database connectivity if a database schema exists. If the check passes, then the installer proceeds to the next step in the process. If the check fails, then an error message is displayed.

- Select the appropriate database options:
  - If a database exists and the connectivity is good, then proceed to Step 11.
  - If no connectivity is detected, then you are prompted to enter new information or to fix the connection. After you do that, click **Next**.

11. On the Authentication Information page, select either the **Oracle Identity Manager Default Authentication** or **SSO Authentication** option. If you select Single Sign-On authentication, then you must provide the header variable used in the Single Sign-On system in the **Enter the header value for SSO Authentication** field. Click **Next**.
12. On the Application Server Selection page, select **IBM WebSphere**, and then click **Next**.
13. On the Cluster Information page, specify whether the server configuration is clustered or nonclustered.

    For a nonclustered installation, select **No**, and then click **Next**.

    If you are deploying in a clustered installation, then select **Yes**, enter the cluster name, and refer to the "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" section on page 9-1 for more information.
14. On the WebSphere Directory Information page, enter the information appropriate for the application server and Java installation:
    a. Enter the full path to the WebSphere installation directory. Ensure that you include `AppServer` in this path, for example: `C:\Program Files\IBM\WebSphere\AppServer`.

       Alternatively, click **Browse** and navigate to the location of the WebSphere installation directory.

    b. Enter the path to the JDK associated with the WebSphere application server. Do not include JRE in this path. For example, a valid path might be: `C:\Program Files\IBM\WebSphere\AppServer\java`.

       Alternatively, click **Browse** and navigate to the location of the JDK installation.

    c. Click **Next**.
15. On the WebSphere Details page, enter the following application server information:
    a. Enter the host name or IP address for the computer on which the application server is running. You can enter `localhost` for a local installation.

    b. Enter the cell name mentioned in the "Obtaining the WebSphere Cell and Node Name" section on page 3-5.

    c. Enter the node name, mentioned in the "Obtaining the WebSphere Cell and Node Name" section on page 3-5.

d. For the WebSphere server name, enter the Oracle Identity Manager server name. The default server name is server1.

e. For the profile name, enter AppSrv01 or the directory name under the *WEBSPHERE_HOME*\profiles\ directory based on the operating system.

f. Click **Next**.

16. Back up the application server when the Application Server Configuration Backup page is displayed, then click **Next** to initiate server installation.

17. On the Summary page, click **Install** to initiate the server software installation.

18. If the installer detects an existing database, then you use that database.

    Select **Yes**, then click **Next**.

    If the existing database is not encrypted, then you are prompted to encrypt it. Select **Yes**, then click **Next**.

19. After Oracle Identity Manager is installed, a message is displayed listing the location of the installer log file and the subsequent steps that you must perform.

    Click **OK** and complete the postinstallation steps listed in the message.

20. On the Completed page, click **Finish** to exit the installer.

    After installing Oracle Identity Manager, follow the instructions in "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server".

5.4 Removing Oracle Identity Manager

To remove an Oracle Identity Manager installation:

1. Stop Oracle Identity Manager if it is running, and stop all Oracle Identity Manager processes.

2. Delete the *OIM_HOME* directory in which you installed Oracle Identity Manager.

6

Installing Oracle Identity Manager on UNIX or Linux

This chapter describes how to install Oracle Identity Manager on a computer running UNIX or Linux in a nonclustered installation.

See Also:

- *Oracle Identity Manager Readme* for information about supported UNIX platforms
- Chapter 9, "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" for information about deploying Oracle Identity Manager in a clustered installation

You must install the Oracle Identity Manager on systems running the application server. Oracle Identity Manager components, such as the Remote Manager, can be installed on separate systems. Each component has its own installer.

This chapter discusses the following topics:

6.1 Installation Prerequisites and Notes

The following is a list of prerequisites and notes for installing Oracle Identity Manager on UNIX or Linux:

- The Oracle Identity Manager Installer program requires at least 200 MB of free space in the home directory of the user installing Oracle Identity Manager. Check the /etc/passwd file to determine the home directory. Note that you cannot work around this requirement by changing the value of the $HOME variable.
- There must be at least 200 MB of free space in the /var/tmp directory.
- Before installing Oracle Identity Manager, you must set the *JAVA_HOME* and PATH variables by following the procedure specific to the operating system that you use. See "Setting Environment Variables" on page 3-4 for instructions.

- The default logging package included by the base RedHat Linux installation causes installation problems and exceptions for Oracle Identity Manager. Before installing Oracle Identity Manager on RedHat Linux, delete the commons-logging-1.0.2 library from the base operating system installation. The commons-logging-1.0.2 library is typically installed with any standard RedHat installation. Also, ensure that you delete the symbolic links in the /usr/share/java/ directory. Deleting these symbolic links will force Oracle Identity Manager to use its own internal logger jar files during installation.
- Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. Use a different Oracle Identity Manager home directory. If you want to reuse the same directory name for the Oracle Identity Manager home directory then back up your previous Oracle Identity Manager home by renaming the original directory.

  Furthermore, all Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory where Oracle Identity Manager is installed.

6.2 Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into your database. You only install the database schema once. It is installed the first time you run the Oracle Identity Manager Installer. Each subsequent time you run the installer to deploy other Oracle Identity Manager components you enter information about the database connection to configure the component for the same schema. If required, contact your database administrator (DBA).

Note: During the schema installation, a log file is created in the *OIM_HOME*/logs directory.

6.3 Installing Documentation

The Oracle Identity Manager documentation is installed automatically in the *OIM_HOME* directory. No special input is required. A full documentation set is installed with each Oracle Identity Manager component.

6.4 Installing Oracle Identity Manager on UNIX or Linux

Oracle Identity Manager for UNIX or Linux is installed through a console mode installer, which supports the following two input methods:

- Choose from among a list of options

  Each option is numbered and accompanied by brackets ([ ]). To select an option, enter its number. Once selected, the associated brackets display an X ([X]).
- Enter information at a prompt.

  To enter information at the prompt, enter the information and press Enter. To accept a default value—default values are enclosed in brackets after a prompt—simply press Enter to accept them.

The installer contains logical sections (panels).

- When you have selected an item from a list of options, enter zero (**0**) to indicate that the desired item has been selected.

- To move to the next installation panel, enter **1**.
- To go back to the previous panel, enter **2**.
- To cancel the installation, enter **3**.
- To redisplay the current panel, enter **5**.

To install Oracle Identity Manager on UNIX or Linux:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. From the console, change directory (`cd`) to the installServer directory on the installation CD and run the install_server.sh by using the following command:

   ```
   sh install_server.sh
   ```

   Note: If you are not installing Oracle Identity Manager from distributed media (CD), you must set the execute bit of all shell scripts in the installServer directory. To set the execute bit for all shell scripts recursively, cd to the installServer directory and run the following command:

   ```
   find . -name "*.sh" -exec chmod u+x {} \;
   ```

   The installer starts in console mode.
3. Choose a language by entering a number from the list of languages.

   Enter **0** to apply the language selection. The Welcome Message panel is displayed.
4. Enter **1** on the Welcome Message panel to display the next panel.

   The Admin User Information panel is displayed.
5. Enter a password you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then enter **1** to move to the next panel.

   The OIM Application Options panel is displayed.
6. Enter **1** on the OIM Application Options panel to display the next panel.

   The Select the Oracle Identity Manager application to install panel is displayed.
7. Select the application to install:
   a. Enter **1** for Oracle Identity Manager.
   b. Enter **2** for the Oracle Identity Manager with Audit and Compliance Module.

      Enter **0** when you are finished and then enter 1 to move to the next section. The Target directory panel is displayed.
8. On the Target directory panel, complete one of the sub-steps that follow:
   - Enter the path to the directory where you want to install Oracle Identity Manager, for example, /opt/oracle/.
   - Enter 1 to move to the next panel.

   If the directory does not exist, you are asked to create it. Enter **y**, for yes. The Database Server Selection panel is displayed.

Note: To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. See *Oracle Identity Manager Readme* to confirm the certified configurations.

When Oracle Identity Manager is installed against an existing database, a warning message will appear indicating the database schema already exists and instructing you to copy the .xldatabasekey file from the existing Oracle Identity Manager installation to the new to the new *OIM_HOME*/xellerate/config directory after you complete the installation process.

Create the new *OIM_HOME*/xellerate/config directory if it does not already exist.

9. Specify the type of database that you are using:
   - Enter **1** to select Oracle Database.
   - Enter **2** to select Microsoft SQL Server.
   - Enter **0** to finish.
   - Enter **1** to move to the next panel.

   The Database Information panel is displayed.
10. Enter your database information:
    - Enter the database host name or IP address.
    - Enter the port number, or accept the default.
    - Enter the SID for the database name.
    - Enter the database user name for the account that Oracle Identity Manager uses to connect to the database.
    - Enter the password for the database account that Oracle Identity Manager uses to connect to the database.
    - Enter **1** to move to the next panel.

      The Authentication Information panel is displayed.
11. Select the authentication mode for the Oracle Identity Manager Web application.
    - Enter **1** for Oracle Identity Manager Default Authentication.
    - Enter 2 for SSO Authentication.
    - Enter **0** when you are finished.

    If you select SSO authentication, you must provide the header variable used in the Single Sign-On system when prompted.

    Enter 1 to move to the next panel.

    The Application Server Selection panel is displayed.
12. Specify your application server type.
    - Enter 4 for IBM WebSphere Application Server.
    - Enter 0 when you are finished.
    - Enter 1 to move to the next panel.

The Cluster Information panel is displayed.

13. Specify if the application server is clustered or not, provide the information specific to your cluster, then perform the following sub-steps:
    - Enter 1 for Yes.
    - Enter 2 for No.
    - Enter 0 when you are finished.
    - If you selected **Yes**, enter the cluster name at the prompt.
    - Enter 1 to move to the next section.

    The Application Server Information panel is displayed.

    Note: The next steps in procedure are for non-clustered, WebSphere-based Oracle Identity Manager installations only. Refer to "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" on page 9-1 for information about installing in a clustered WebSphere environment.

14. Enter the application server information at the prompts:
    a. Specify the path to the application server or press the Enter key to accept the default.
    b. Specify the path to the application server's JDK directory or press the Enter key to accept the default.
    c. Enter 1 to move to the next section.
15. Enter the login information for the WebSphere server:
    a. Enter the Application Server host name or IP address.
    b. Enter the WebSphere Cell Name.
    c. Enter the WebSphere Node Name.
    d. Enter the WebSphere Server Name.
    e. Enter the Profile Name.
    f. Enter 1 to move to the next section.
16. When a message is displayed warning you to back up your application server, proceed to back up your installation, then enter 1 to move to the next section.
17. On the Installation summary information page, verify the information displayed, then do one of the following:
    - Enter **2** to go back and make changes.
    - Enter 1 to start the installation.
18. After Oracle Identity Manager installs, the Completed panel is displayed. Enter 3 to finish and exit.

After installing Oracle Identity Manager, follow the instructions in Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server".

6.5 Removing Oracle Identity Manager

To remove an Oracle Identity Manager installation:

1. Stop Oracle Identity Manager if it is running and stop all Oracle Identity Manager processes.
2. Delete the *OIM_HOME* directory where you installed Oracle Identity Manager.

7

Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server

After installing Oracle Identity Manager, perform the postinstallation tasks documented in this chapter that are appropriate for your deployment before using the application. Depending on the Oracle Identity Manager deployment, you might choose not to perform some of these tasks.

The postinstallation tasks are discussed in the following topics:

7.1 Default JMS Queue Details

Previously, Oracle Identity Manager used a single JMS queue (named xlQueue) for all asynchronous operations including requests, reconciliation, attestation, and offline tasks. From release 9.1.0 onward, by default, Oracle Identity Manager uses separate JMS queues for specific operations to optimize JMS queue processing. The following list shows the JMS queues in the default configuration and indicates the operation related to each queue:

- `xlQueue` (for request operations)
- `xlReconQueue` (for reconciliation operations)
- `xlAuditQueue` (for auditing operations)
- `xlAttestationQueue` (for attestation operations)
- `xlProcessQueue` (for use in a future release)

7.2 Increasing the JMS Message Threshold

You must increase the default JMS message threshold of 50000 to 999999 on all the JMS queues.

To increase the default JMS message threshold for each JMS queue:

1. Log in to the WebSphere Administrative Console.
2. Click **Service Integration**, **Buses**, **XellerateBus**, **Destinations**, ***QUEUE_NAME***, **Queue Points**, and ***QUEUE_POINT_NAME***.
3. In the **High Message Threshold** field, enter 999999.

Repeat Steps 2 through 3 for all the JMS queues.

7.3 Configuring WebSphere on Nondefault Ports

To run Oracle Identity Manager on IBM WebSphere Application Server by using nondefault ports (not 80, 443, or 9080), you must add the port mapping information for the server by using the WebSphere administrative console. Add the port mapping for the HTTP transport for the nondefault server by using the WebSphere administrative console, as described in the following sections.

7.3.1 Configuring WebSphere on Nondefault HTTP Port

To use a nondefault HTTP port:

1. Select **Environment**, **Virtual Host**, **default_host**, and then select **Host Alias**.
2. Click **New**.
3. Enter the host name and port number.

> **Note:** Setting the Virtual Host, by default, does not include the nonstandard ports for a WebSphere configuration. You must set the Virtual Host for nonstandard server installation and clustered environment installation.

4. Change the `<ApplicationURL>` tag in `xlclient\config\xlconfig.xml` to the correct HTTP port.
5. Restart the application server you used to install Oracle Identity Manager.

7.3.2 Configuring WebSphere on Nondefault Naming Service Port

To use a nondefault naming service port:

1. In the WebSphere Administrative Console, click **Server**, select **Application Server**, select *SERVER_NAME*, and then select **Ports** under **Communication**. Make a note of the BOOTSTRAP_ADDRESS.

   The page displays the host name and port number. The default port is `2809`.

   When installing on a nondefault port, the xlconfig.xml file must be modified even if the installation is on server1. In a clustered installation, the xlconfig.xml file must always be modified.

   Note: The default server, server1, needs the configuration file, xlconfig.xml as well as all other servers (nondefault) in the cell to share the same security information.

2. Edit the discovery port settings in the following files:
   - `xellerate\config\xlconfig.xml`
   - `xlclient\config\xlconfig.xml`

7.4 Configuring the ORB Service

When a business transaction, for example, searching for multiple requests or users, returns a large dataset object (greater than 500KB), it can cause the system to throw an exception. When this happens by using WebSphere, CORBA_NO_MEMORY is recorded in the WebSphere log file and System Error is displayed as an error message window in the Oracle Identity Manager Administrative and User Console.

WebSphere documentation explains that this exception is thrown because an Application Server can record totally out of heap space or insufficient heap space to satisfy allocation request when the Java virtual machine is unable to allocate a block contiguous space on the heap to allocate a large object.

To avoid this exception, you must enable WebSphere to pass parameters by reference through ORB. If enabled, ORB passes parameters by reference, instead of by value, which avoids making an object copy. If you do not enable Pass by reference, the parameters are copied to the stack before every remote method call is made.

Perform the following steps to enable the Pass by Reference parameter for the ORB Service:

1. Log in to the WebSphere Administrative Console.
2. Select **Servers**, then **Application Servers**, then *SERVER_NAME*, and then **ORB Service** under Container Services. The ORB Service window is displayed.
3. Locate the Pass by reference parameter and select the option for the parameter to enable it.
4. Click **Apply**.
5. Save the service settings.

7.5 Changing Keystore Passwords

During installation, the passwords for the Oracle Identity Manager keystores are set to `xellerate`. The Installer scripts and installation log contain this default password. It is strongly recommended that you change the keystore passwords for all production installations.

To change the keystore passwords you must change the storepass of .xlkeystore and the keypass of the xell entry in .xlkeystore, and these two values must be identical. Use the keytool and the following steps to change the keystore passwords:

1. Open a command prompt on the Oracle Identity Manager host computer.
2. Navigate to the *OIM_HOME*\xellerate\config directory.
3. Run the keytool with the following options to change the storepass:

   ```
   JAVA_HOME\jre\bin\keytool -storepasswd -new new_password -storepass xellerate
   -keystore .xlkeystore -storetype JKS
   ```

4. Run the keytool with the following options to change the keypass of the xell entry in .xlkeystore:

   ```
   JAVA_HOME\jre\bin\keytool -keypasswd -alias xell -keypass xellerate -new
   new_password -keystore .xlkeystore -storepass new_password
   ```

> **Note:** Replace *new_password* with the same password entered in step 3.

Table 7–1 lists the options used in the preceding example of keytool usage.

Table 7–1 Command Options for the keytool Utility

Option	Description
JAVA_HOME	Location of the Java directory associated with the application server
new_password	New password for the keystore
-keystore *option*	Keystore whose password you are changing (.xlkeystore for Oracle Identity Manager or .xldatabasekey for the database)
-storetype *option*	JKS for .xlkeystore and JCEKS for .xldatabasekey

5. In a text editor, open the *OIM_HOME*\xellerate\config\xlconfig.xml file.
6. Edit the <xl-configuration>.<Security>.<XLPKIProvider>.<KeyStore> section, <xl-configuration>.<Security>.<XLPKIProvider>.<Keys> section, and the <RMSecurity>.<KeyStore> section to specify the keystore password as follows:

> **Note:** Change the <XLSymmetricProvider>.<KeyStore> section of the configuration file to update the password for the database keystore (.xldatabasekey).

   - Change the password tag to encrypted="false".
   - Enter the password, for example:

   ```
   <Security>
   <XLPKIProvider>
   <KeyStore>
         <Location>.xlkeystore</Location>
         <Password encrypted="false">new_password</Password>
         <Type>JKS</Type>
   ```

```
      <Provider>com.ibm.crypto.provider.IBMJCE</Provider>
</KeyStore>
<Keys>
<PrivateKey>
<Alias>xell</Alias>
<Password encrypted="false">new_password</Password>
</PrivateKey>
</Keys>
<RMSecurity>
<KeyStore>
<Location>.xlkeystore</Location>
<Password encrypted="false">new_password</Password>
<Type>JKS</Type>
<Provider>com.ibm.crypto.provider.IBMJCE</Provider>
</KeyStore>
```

7. Save and close the xlconfig.xml file.
8. Restart the application server.

   When you stop and start the application server, a backup of the configuration file is created. The configuration file with the new password is read in, and the password is encrypted in the file.
9. If all of the preceding steps have succeeded, you can delete the backup file.

Note: On UNIX or Linux, you might also want to clear the command history of the shell by using the following command:

```
history -c
```

7.6 Setting Log Levels

Oracle Identity Manager uses log4j for logging. Logging levels are configured in the logging properties file, *OIM_HOME*/xellerate/config/log.properties. By default, Oracle Identity Manager is configured to provide output at the Warning level except for DDM, which is configured to provide output at the Debug level by default. You can change the log level universally for all components or for an individual component.

The following is a list of the supported log levels, appearing in descending order of information logged. DEBUG logs the most information and FATAL logs the least information.

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

Oracle Identity Manager components are listed in the *OIM_HOME*\xellerate\config\log.properties file in the XELLERATE section, for example:

```
log4j.logger.XELLERATE=WARN
log4j.logger.XELLERATE.DDM=DEBUG
log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=DEBUG
```

```
log4j.logger.XELLERATE.SERVER=DEBUG
log4j.logger.XELLERATE.RESOURCEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.REQUESTS=DEBUG
log4j.logger.XELLERATE.WORKFLOW=DEBUG
log4j.logger.XELLERATE.WEBAPP=DEBUG
log4j.logger.XELLERATE.SCHEDULER=DEBUG
log4j.logger.XELLERATE.SCHEDULER.Task=DEBUG
log4j.logger.XELLERATE.ADAPTERS=DEBUG
log4j.logger.XELLERATE.JAVACLIENT=DEBUG
log4j.logger.XELLERATE.POLICIES=DEBUG
log4j.logger.XELLERATE.RULES=DEBUG
log4j.logger.XELLERATE.DATABASE=DEBUG
log4j.logger.XELLERATE.APIS=DEBUG
log4j.logger.XELLERATE.OBJECTMANAGEMENT=DEBUG
log4j.logger.XELLERATE.JMS=DEBUG
log4j.logger.XELLERATE.REMOTEMANAGER=DEBUG
log4j.logger.XELLERATE.CACHEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.ATTESTATION=DEBUG
log4j.logger.XELLERATE.AUDITOR=DEBUG
```

To set Oracle Identity Manager log levels, edit the logging properties in the *OIM_HOME*\xellerate\config\log.properties file as described in the following procedure.

To configure log levels:

1. In a text editor, open the *OIM_HOME*\xellerate\config\log.properties file.

   This file contains a general setting for Oracle Identity Manager and specific settings for the components and modules that comprise Oracle Identity Manager.

   By default, Oracle Identity Manager is configured to output at the Warning level:

   ```
   log4j.logger.XELLERATE=WARN
   ```

   This is the general value for Oracle Identity Manager. Individual components and modules are listed by following the general value in the properties file. You can set individual components and modules to different log levels. The log level for a specific component overrides the general setting.

2. Set the general value to the desired log level.

3. Set other component log levels as desired.

   Individual components or modules can have different log levels. For example, the following values set the log level for the Account Management module to INFO, while the server is at DEBUG and the rest of Oracle Identity Manager is at the WARN level.

   ```
   log4j.logger.XELLERATE=WARN
   log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO
   log4j.logger.XELLERATE.SERVER=DEBUG
   ```

4. Save the changes.

5. Restart the application server so that the changes take effect.

7.7 Enabling Single Sign-On (SSO) for Oracle Identity Manager

The following procedure describes how to enable Single Sign-On for Oracle Identity Manager with ASCII character logins. To enable Single Sign-On with non-ASCII

character logins, use the following procedure, but include the additional configuration setting described in step 4.

> **See Also:** *Oracle Identity Manager Best Practices Guide* for more information about configuring Single Sign-On for Oracle Identity Manager with Oracle Access Manager.

> **Note:** Header names comprised only of alphabetic characters are certified. Oracle recommends that not using special characters or numeric characters in header names.

To enable Single Sign-On for Oracle Identity Manager:

1. Stop the application server gracefully.
2. In a text editor, open the *OIM_HOME*\xellerate\config\xlconfig.xml file.
3. Locate the following Single Sign-On configuration. The following are the default settings without Single Sign-On:

```
<web-client>
<Authentication>Default</Authentication>
<AuthHeader>REMOTE_USER</AuthHeader>
</web-client>
```

4. Edit the Single Sign-On configuration to be the following, and replace *SSO_HEADER_NAME* with the appropriate header configured in your Single Sign-On system:

```
<web-client>
<Authentication>SSO</Authentication>
<AuthHeader>SSO_HEADER_NAME</AuthHeader>
</web-client>
```

   To enable Single Sign-On with non-ASCII character logins, you must include a decoding class name to decode the non-ASCII header value. Add the decoding class name and edit the Single Sign-On configuration as follows:

```
<web-client>
<Authentication>SSO</Authentication>
<AuthHeader>SSO_HEADER_NAME</AuthHeader>
<AuthHeaderDecoder>com.thortech.xl.security.auth.CoreIDSSOAuthHeaderDecoder</Au
thHeaderDecoder>
</web-client>
```

   Replace *SSO_HEADER_NAME* with the appropriate header configured in your Single Sign-On system.

5. Change the application server and Web server configuration to enable Single Sign-On by referring to the application and Web server vendor documentation.
6. Restart the application server.

7.8 Configuring Custom Authentication

This section describes how to use custom authentication solutions with Oracle Identity Manager.

Oracle Identity Manager deploys a Java Authentication and Authorization Service (JAAS) module to authenticate users. For unattended logins, which require offline message processing and scheduled task execution, Oracle Identity Manager uses signature-based authentication. Although you can use JAAS to handle signature-based authentication, you can create a custom authentication solution to handle standard authentication requests.

Note: The Oracle Identity Manager JAAS module must be deployed on the application server and must be the first invoked authenticator.

To enable custom authentication on WebSphere application server, you use the WebSphere Administrative Console to define a property named `customAuthentication` in the Custom Properties section of the Custom User Registry, as follows:

1. Log in to the WebSphere Administrative Console
2. Expand **Security** and **User Registries**, and then click **Custom**. The Custom Properties page is displayed.
3. On the Custom Properties page, click **New** and define a property named **customAuthentication**. When you define the property, specify the name of a custom authentication class that implements `com.ibm.websphere.security.UserRegistry`, and also provide any required initialization parameters.
4. Restart the WebSphere application server.

7.8.1 Protecting the JNDI Namespace

When you specify a custom authentication solution, you must also protect the Java Naming and Directory Interface (JNDI) namespace to ensure that only designated users have permission to view resources. The primary purpose of protecting the JNDI namespace is to protect Oracle Identity Manager from any malicious applications that might be installed in the same application server instance. Even if no other applications, malicious or otherwise, are installed in the same application server instance as Oracle Identity Manager, you must protect your JNDI namespace as a routine security measure.

To configure Oracle Identity Manager to access a protected JNDI namespace, perform the following steps:

1. Open the *OIM_HOME*`/config/xlconfig.xml` file in a text editor and add the following elements to the `<Discovery>` element:

```
<java.naming.security.principal>
<java.naming.security.credentials>
```

2. To optionally encrypt the JNDI password, add an encrypted attribute that is assigned a value of true to the `<java.naming.security.credentials>` element, and assign the password as the value of the element, as follows:

```
<java.naming.security.credentials
  encrypted="true">password</java.naming.security.credentials>
```

3. Add the following elements to the `<Scheduler>` element:

```
<CustomProperties>
  <org.quartz.dataSource.OracleDS.java.naming.security.principal>user
```

```
  </org.quartz.dataSource.OracleDS.java.naming.security.principal>
  <org.quartz.dataSource.OracleDS.java.naming.security.credentials>pwd
  </org.quartz.dataSource.OracleDS.java.naming.security.credentials>
</CustomProperties>
```

4. Restart the server.

7.9 Increasing the Transaction Timeout

You have to increase the transaction timeout values for WebSphere Application Server because the default values can be low for certain transactions. Oracle recommends that the values as specified in the following steps.

> **Note:** Depending on the specific requirements, the values might require revision in the future.

1. Log in to the WebSphere Administrative Console.
2. Select **Servers**, **Application Servers**, *SERVER_NAME*, and then select **Transaction Services** under Container Services.
3. Enter **1200** for total transaction lifetime timeout.
4. Enter **1200** for maximum transaction timeout.
5. Save the service settings.
6. Restart the servers.

> **Note:** In the cluster environment, you must repeat the steps for all the available WebSphere servers in the cluster.

7.10 Increasing the Authentication Expiration

Be default the websphere expires the authentication information based on the timeout configuration. By default timeout is set at 120 minutes. Note that this might not be enough, if you are planning to run a long reconciliation activity or any other scheduled tasks. Therefore, timeout must be increased to a suitable value in minutes.

To increase the authentication expiration:

1. Log on to the WebSphere Administrative Console.
2. Click **Security**.
3. Select **Secure administration, applications, and infrastructure**.
4. Select **Authentication mechanisms and expiration**.
5. Enter the value for **Timeout value for forwarded credentials between servers** in minutes.

7.11 Selecting the Oracle 10*g* Data Store Helper Class

Perform the following steps to change the default Oracle 9*i* Data Store Helper class to the Oracle 10*g* Data Store Helper class:

1. Log on to WebSphere Administrative Console.

2. Select **Resources**, **JDBC**, **Data Sources**, and then select **Non XA DataSource**.
3. Select **Oracle 10g data store helper** in the **Data store helper class name** field.
4. Click **OK**, and then click **Save**.
5. Select **Resources**, **JDBC**, **Data Sources**, and then select **XA DataSource**.
6. Select **Oracle 10g data store helper** in the **Data store helper class name** field.
7. Click **OK**, and then click **Save**.

7.12 Setting the Compiler Path for Adapter Compilation

To compile adapters or import Deployment Manager XML files that have adapters, you must set the compiler path. To set the compiler path for adapter compilation, you must first install the Design Console. Refer to Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" for instructions on installing the Design Console and then setting the compiler path for adapter compilation.

7.13 Deploying the SPML Web Service

Organizations can have multiple provisioning systems that exchange information about the modification of user records. In addition, there can be applications that interacts with multiple provisioning systems. The SPML Web Service provides a layer over Oracle Identity Manager to interpret SPML requests and convert them to Oracle Identity Manager calls.

The SPML Web Service is packaged in a deployable Enterprise Archive (EAR) file. This file is generated when you install Oracle Identity Manager.

Because the EAR file is generated while you install Oracle Identity Manager, a separate batch file in the Oracle Identity Manager home directory runs the scripts that deploy the SPML Web Service on the application server on which Oracle Identity Manager is running. You must run the batch file to deploy the SPML Web Service.

For details about the SPML Web Service, see Chapter 12, "The SPML Web Service" in *Oracle Identity Manager Tools Reference*.

7.14 Tuning JDBC Connection Pools

To implement the tuning for the JDBC connection pools used by Oracle Identity Manager:

Note: It is strongly recommended that you implement the suggested tuning for the JDBC connection pools used by Oracle Identity Manager. This can be further tuned based on the application usage.

---

1. Log on to WebSphere Administrative Console.
2. Select Resources, JDBC, Data Sources, and then select Non XA DataSource. Select Connection pool properties under Additional properties. And enter/ensure the following values.

```
Minimum connections: 30
Maximum connections: 50
```

3. Click **OK**, and then click **Save**.

4. Select Resources, JDBC, Data Sources, and then select XA DataSource. Select Connection pool properties under Additional properties. And enter/ensure the following values.

```
Minimum connections: 30
Maximum connections: 50
```

5. Click **OK**, and click **Save**.

7.15 Copying the sqljdbc.jar File

Copy the sqljdbc.jar file from the C:\jdbc_install_folder\ directory to the *WEBSPHERE_HOME*/lib/ directory.

Note:

- For a cluster installation of Oracle Identity Manager, copy the sqljdbc.jar file to the *NDM_HOME*/lib directory in all the cluster nodes.
- If the sqljdbc.jar is not copied to the *WEBSPHERE_HOME*/lib/ directory, then Oracle Identity Manager fails to start.

8

Starting and Stopping Oracle Identity Manager

This chapter describes how to start and stop Oracle Identity Manager, and how to access the Administrative and User Console. This chapter contains the following topics:

> **Note:** You must complete all relevant postinstallation steps before starting Oracle Identity Manager. Refer to the "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server" section on page 7-1 for more information.

8.1 Removing Backup xlconfig.xml Files After Starting or Restarting

After you start any Oracle Identity Manager component for the first time, or after you change any passwords in the xlconfig.xml file, Oracle Identity Manager encrypts and saves the passwords. Oracle Identity Manager also creates a backup copy of the xlconfig.xml file before saving changes to the file. These backup files contain old passwords in plaintext. The backup file are named xlconfig.xml.*x*, where *x* is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on.

> **Note:** You must remove these backup files after starting any Oracle Identity Manager component for the first time, or on restarting after changing any passwords in xlconfig.xml once you have established that the new password is working properly.

8.2 Starting Oracle Identity Manager

This section describes how to start Oracle Identity Manager on Microsoft Windows, UNIX, or Linux.

To start Oracle Identity Manager:

1. Verify that your database is up and running.

2. Start Oracle Identity Manager by starting the WebSphere application server. Run one of the following scripts appropriate for your operating system to start IBM WebSphere Application Server and Oracle Identity Manager:

   To start an administrative server on Microsoft Windows, run the *WEBSPHERE_HOME*\profiles*PROFILE_NAME*\bin\startServer.bat *SERVER_NAME* script.

   To start an administrative server on UNIX or Linux, run the *WEBSPHERE_HOME*/profiles/*PROFILE_NAME*/bin/startServer.sh *SERVER_NAME* script.

8.3 Stopping Oracle Identity Manager

This section describes how to stop Oracle Identity Manager gracefully on Microsoft Windows, UNIX, or Linux. To stop Oracle Identity Manager gracefully, you stop the WebSphere application server by running one of the following scripts appropriate for the operating system.

On Microsoft Windows:

WEBSPHERE_HOME\profiles*PROFILE_NAME*\bin\stopServer.bat *SERVER_NAME*

On UNIX or Linux:

WEBSPHERE_HOME/profiles/*PROFILE_NAME*/bin/stopServer.sh *SERVER_NAME*

8.4 Accessing the Administrative and User Console

After starting the WebSphere application server and Oracle Identity Manager, you can access the Administrative and User Console by performing the following steps:

1. Navigate to the following URL by using a Web browser:

   http://*hostname*:*port*/xlWebApp

   In this URL, *hostname* represents the name of the computer hosting the application server and *port* refers to the port on which the server is listening. The default port number for WebSphere is 9080.

   Note: The application name, xlWebApp, is case-sensitive.

   For example:

   http://localhost:9080/xlWebApp

2. After the Oracle Identity Manager login page is displayed, log in with your user name and password.

8.5 Using Diagnostic Dashboard to Verify Installation

The Diagnostic Dashboard verifies each component in your postinstallation environment by testing for:

- A trusted store
- Single sign-on configuration
- Messaging capability

- A task scheduler
- A Remote Manager

The Diagnostic Dashboard also checks for all supported versions of components along with their packaging.

> **See Also:** The "Using the Diagnostic Dashboard" section on page 2-5 for more information about installing and using the Diagnostic Dashboard

9

Deploying Oracle Identity Manager in a Clustered WebSphere Configuration

This chapter describes how to deploy Oracle Identity Manager in a clustered IBM WebSphere Application Server environment.

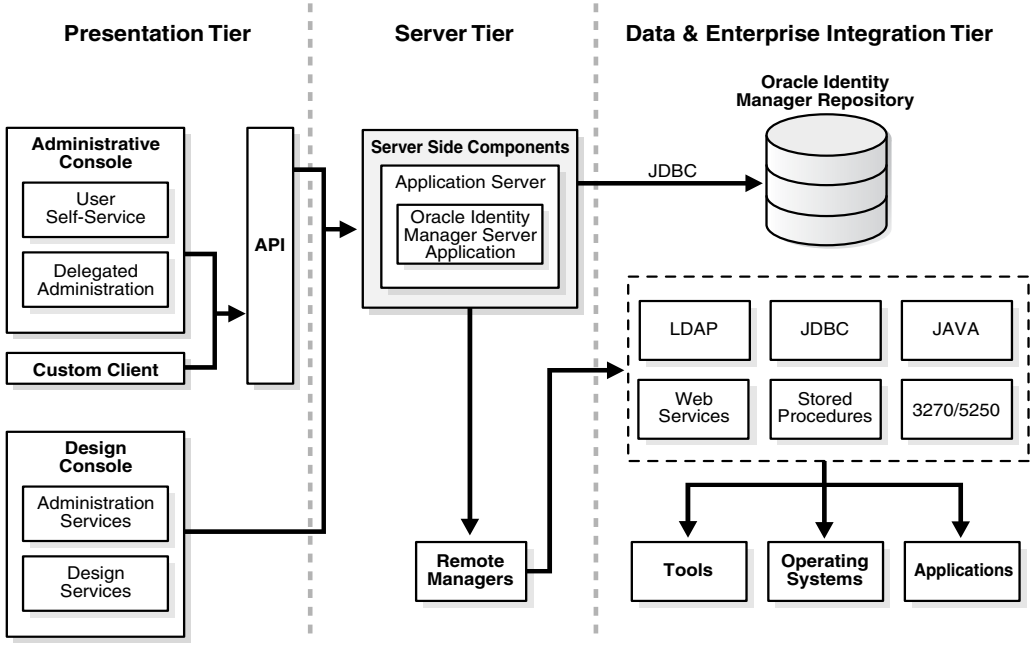
This chapter discusses the following topics:

Caution: Deploying an application in a clustered environment is a highly complex procedure. This document assumes that you have expertise in installing and using applications in a WebSphere cluster. These instructions provide the Oracle Identity Manager-specific details only. They are not complete instructions for setting up a WebSphere cluster. For more information about clustering, refer to WebSphere documentation.

9.1 About Clustered WebSphere Configurations

Figure 9–1 is the run-time representation of most of the server components after Oracle Identity Manager is installed by using the instructions given in this section. The diagram focuses mainly on the JMS architecture of the clustered installation.

Figure 9–1 Run-Time Representation of Oracle Identity Manager Components



Note: The WebSphere cluster architecture diagram is an overview and does not represent the complete architecture.

For a clustered environment, several host computers are required. The instructions in this chapter describe using 4+n computers and are primarily focussed on Microsoft Windows. Your configuration might vary. Table 9–1 describes the entities needed for a cluster, the computers that they run on, and the software required for the entities. Host computers and entities are labeled descriptively.

Table 9–1 WebSphere-based Oracle Identity Manager Cluster Host Computers

Host Computer	Entities	Software	Description
NDM_HOST	XL_MODEL_NODE XL_MODEL_SERVER	WebSphere Oracle Identity Manager	Use the model node and server as a template. Configure the model server and copy it to the nodes for each application server in the cluster. **Note:** The model node is not part of the cluster.
IIS_HOST	IIS server	IIS WebSphere Plug-in	This is the IIS Web server. The IIS server acts as the front end to the WebSphere cluster and handles the load balancing. Install IIS and the WebSphere plug-in on this computer.
XL_NODEn_HOST	XL_NODEn XL_CLUSTER	WebSphere Oracle Identity Manager	Each application server in the cluster runs Oracle Identity Manager. The application servers run on one or more node host computers. Replace n with the node number, such as XL_NODE1. You can have more than one application server for each node host computer.
XL_JMS_HOST	XL_JMS_NODE XL_JMS_CLUSTER	WebSphere	Application servers created in this cluster are used for JMS message handling. Oracle recommends that at least two application servers are created in this cluster for failover capabilities for the JMS message processing.

9.2 Overview of Setting Up a WebSphere Oracle Identity Manager Cluster

This section discusses the high-level tasks involved in setting up WebSphere Oracle Identity Manager cluster.

> **Note:** Before setting up a clustered environment for WebSphere, ensure that all cluster member computers have their clock synchronized so that the Scheduler can operate properly.

To set up Oracle Identity Manager for a WebSphere cluster:

1. Install and upgrade the WebSphere Application Server Network Deployment on NDM_HOST.

   Refer to the "Installing WebSphere Application Server for a Cluster" section on page 9-6 for information about steps 1 and 2.

2. Install and upgrade WebSphere Application Server Network Deployment on each node host (XL_NODE1_HOST, XL_NODE2_HOST, and so on.)

3. Install and upgrade WebSphere Application Server Network Deployment on XL_JMS_HOST.

4. Add the XL_MODEL_NODE to the Network Deployment Manager on NDM_HOST.

   Refer to the "Adding the Model Node to the Network Deployment Manager" section on page 9-13 for information about adding the model node to the Network Deployment Manager.

5. Create the XL_MODEL_SERVER on the XL_MODEL_NODE.

   Refer to the "Creating the Model Server" section on page 9-14 for information about creating the modal server.

6. Create the XL_CLUSTER.

   Refer to the "Creating the XL_CLUSTER" section on page 9-14 for information about creating the XL_CLUSTER.

7. Create the XL_JMS_CLUSTER.

   Refer to the "Creating the JMS CLUSTER" on page 9-15 for information about creating the JMS cluster.

8. Prepare the database.

   Refer to the "Using an Oracle Database for Oracle Identity Manager" section on page 4-1 or the "Using a Microsoft SQL Server Database for Oracle Identity Manager" section on page 4-7 for information about preparing the database.

9. Install Oracle Identity Manager on NDM_HOST.

   Refer to the "Installing Oracle Identity Manager on the Network Deployment Manager" section on page 9-16 for information about installing Oracle Identity Manager on NDM_HOST.

10. Set up the WebSphere custom registry on NDM_HOST.

11. To add a node, copy the *OIM_HOME* directory from NDM_HOST to XL_NODE1_HOST.

    Refer to the "Adding Nodes to WebSphere Cell" section on page 9-21 for information about steps 11 through 16.

12. Add Node XL_NODEn, such as XL_NODE1, to the Network Deployment Manager.

13. Add Node XL_JMS_NODE to the Network Deployment Manager.

14. Create a server, such as XL_SERVER_ON_NODE1, on XL_NODE1 as a cluster member.

15. Create JMS servers, such as XL_JMS_SERVER1 and XL_JMS_SERVER2, on XL_JMS_NODE as a cluster member of XL_JMS_CLUSTER.

16. Set up virtual host information for the server.

17. Repeat steps 14 through 16 for each server you want to add to the node.

18. Repeat steps 11 through 16 for each node you want to add to the cluster.

19. Get the JNDI URL and update the JNDI references in the xlconfig.xml file associated with each server.

    Refer to the "Updating the JNDI References" section on page 9-26 for information about updating the JNDI references.

20. Install the WebSphere Plug-in on IIS_HOST.

Refer to the "Installing the WebSphere Plug-in for IIS" section on page 9-7 for information about installing the WebSphere plug-in for IIS.

21. Set up the IIS server.

    Refer to the "Configuring the IIS Plug-in" section on page 9-30 for information about configuring the IIS plug-in.

22. Set up the Design Console.

    Refer to the "Postinstallation Requirements for the Design Console" section on page 10-3 for information about setting up the Design Console.

23. Perform the postinstallation tasks after deploying Oracle Identity Manager in your cluster.

    Refer to the "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server" section on page 7-1 for information about the postinstallation tasks that you perform after deploying Oracle Identity Manager in the cluster.

9.2.1 WebSphere Software Host Requirements

The software requirements for WebSphere host are:

- WebSphere host (and component) computers require the IBM JVM. Conflicts can arise if any of the following is true:
  - Other JVM instances exist in PATH.
  - JAVA_HOME or CLASSPATH point to anything other than an IBM JVM 1.5.x installation.
- If you have any other JVMs on the cluster computers, remove (uninstall) them before proceeding.
- Unset the JAVA_HOME, ANT_HOME, and CLASSPATH variables.
- For a full WebSphere installation, you need the Application Server and Application Client installers.

9.3 Backing Up the Configurations

Oracle recommends that at various points during the cluster setup, you make backups of the various components. This lets you roll back changes rather than restart the entire process. WebSphere provides a script (backupconfig.bat or backupconfig.sh) that makes a compressed (zip) file of the configuration settings. This script takes the backup file name with complete path as an argument.

The configuration backup script stops the Node Manager as well as all the nodes on which it is run. It is possible to get backups without stopping the nodes or Node Manager. However, Oracle recommends that you stop them before making the configuration backups. After completing the configuration backups, ensure that you restart the Node Manager (startmanager.bat or startmenager.sh) as well as the Nodes (startnode.bat or startnode.sh).

Note: After Oracle Identity Manager is installed and the custom registries are created, you must specify the user name and password to start the Node Manager or the nodes.

When setting up the cluster, run the script at various times to save the current settings.

To back up your server configurations:

1. On the server host computer, create backup directories for the configurations you are backing up.

   For example, to make a back up of the Node Manager configuration, use the following command to create a directory for the backup:

   ```
   mkdir C:\WAS_Backups\PreXL\NodeManagerConfig
   ```

   Or:

   ```
   mkdir /opt/WAS_Backups/PreXL/NodeManagerConfig
   ```

2. Change directories to the application server bin directory. For example:

   ```
   cd WEBSPHERE_HOME\profiles\PROFILE_NAME\bin
   ```

3. Run backupconfig.bat or backupconfig.sh and specify a file name that is in the backup directory you created. For example:

   ```
   backupconfig.bat
   c:\WAS_Backups\PreXL\NodeManagerConfig\ConfigBkp.zip
   ```

   Or:

   ```
   ./backupconfig.sh/opt/WAS_Backups/PreXL/NodeManagerConfig/ConfigBkp.zip
   ```

9.4 Installing WebSphere Application Server for a Cluster

To install and upgrade WebSphere application server, you need the WebSphere installer and upgrade scripts. Ensure that the host meets the WebSphere requirements. Refer to the "WebSphere Software Host Requirements" section on page 9-5 for information about WebSphere host system requirements.

Install WebSphere on:

- NDM_HOST for the model node XL_MODEL_NODE and Deployment Manager Node XL_MANAGER_NODE
- All node host computers such as XL_NODE1_HOST and XL_NODE2_HOST
- JMS node host computer such as XL_JMS_HOST

For each WebSphere host computer:

1. Install the server.

   Refer to the "Installing WebSphere Application Server" section on page 9-7 for information.

2. Upgrade the server.

   Refer to the "Upgrading the WebSphere Server" section on page 9-7 for information.

3. Set the environment variables.

   Refer to the "Setting Environment Variables" section on page 9-7 for information.

4. Create profiles.

   Refer to the "Creating WebSphere Profiles" section on page 9-8 for information.

5. Set the memory size.

   Refer to the "Setting JVM Memory and Arguments" section on page 9-11 for information.

6. Enable SOAP communications.

   Refer to the "Enabling SOAP Communication to WebSphere" section on page 9-12 for information.

7. Verify the installation.

   Refer to the "Verifying Installation" section on page 9-12 for information.

8. Create Backups.

   Refer to the "Creating Backups" section on page 9-12 for information.

9.4.1 Installing WebSphere Application Server

Install the supported version of the WebSphere Application Server Network Deployment. When installing, after you select the installation directory, choose the **None** option for WebSphere Application Server environments. You can create your profile later, allowing for flexibility in naming of the servers and nodes.

Important: During the installation, you must clear the **Enable administrative security** option on the Enable Administrative Security page of the WebSphere installer. By default, the **Enable administrative security** option is selected.

9.4.2 Upgrading the WebSphere Server

To upgrade the WebSphere server:

1. After you install the WebSphere Application Server Network Deployment Manager, update it to the fix packs from IBM that are supported by Oracle Identity Manager.
2. Upgrade the JDK for WebSphere server.

   See Also: *Oracle Identity Manager Readme* for the minimum certified versions of WebSphere fix packs and JDK fixes required by Oracle Identity Manager. Oracle Identity Manager supports all JDK fixes and WebSphere fix packs on top of the minimum certified versions.

9.4.3 Setting Environment Variables

The following environment variable settings are necessary for Oracle Identity Manager Installer:

- Ensure that the `JAVA_HOME` system variable is set to the appropriate JDK. On Microsoft Windows, Solaris, and Linux, set `JAVA_HOME` to Sun JDK. On AIX, set `JAVA_HOME` to the IBM JDK (bundled with IBM WebSphere).

  See Also: *Oracle Identity Manager Readme* for information about certified JDK versions

- Remove the `ANT_HOME` system variable if it is defined.

- For Microsoft Windows, Solaris, and Linux, ensure that the Sun JDK is being used when a Java command is run. To do this, include the `/java/jre/bin/` directory of the Sun JDK installation in the `PATH` ahead of all other path entries. For example:

  Microsoft Windows:

  ```
  set PATH=SUN_JDK_HOME\jre\bin;%PATH%
  ```

  Solaris or Linux

  ```
  export PATH=SUN_JDK_HOME/jre/bin:$PATH
  ```

- For AIX, ensure that the IBM JDK (bundled with IBM WebSphere) is being used when a Java command is run. To do this, include the `/java/jre/bin/` directory of IBM JDK installation in the PATH ahead of all other path entries. For example:

  ```
  export PATH=IBM_JDK_HOME/jre/bin:$PATH
  ```

9.4.4 Creating WebSphere Profiles

Create the following profiles, either by using the *WEBSPHERE_HOME*`/bin/manageprofiles` command or using WebSphere's Profile Management tool. The following sections provide information for both the methods:

- XL_MANAGER_PROFILE for Deployment Manager on NDM_HOST
- XL_MODEL_PROFILE for model node (XL_MODEL_NODE) on NDM_HOST
- XL_JMS_PROFILE for model node (XL_JMS_NODE) on JMS_HOST
- XL_NODEn_PROFILE for XL_NODEn on NODEn_HOST

> **Note:** When you create profiles, substitute appropriate values for *WEBSPHERE_HOME* and *HOST_NAME* variables. This applies to all instances of profile creation.

XL_MANAGER_PROFILE for Deployment Manager on NDM_HOST

Create XL_MANAGER_PROFILE, run the *WEBSPHERE_HOME*/bin/manageprofiles command on NDM_HOST, as shown:

For Microsoft Windows:

```
WEBSPHERE_HOME\bin\manageprofiles.bat -create
-templatePath "WEBSPHERE_HOME\profileTemplates\dmgr" -profileName
XL_MANAGER_PROFILE -profilePath "WEBSPHERE_HOME\profiles\XL_MANAGER_PROFILE"
-nodeName XL_MANAGER_NODE -cellName XL_CELL -hostname HOST_NAME
```

For UNIX:

```
WEBSPHERE_HOME/bin/manageprofiles.sh -create
-templatePath "WEBSPHERE_HOME/profileTemplates/dmgr"
-profileNameXL_MANAGER_PROFILE -profilePath
"WEBSPHERE_HOME/profiles/XL_MANAGER_PROFILE"
-nodeName XL_MANAGER_NODE -cellName XL_CELL -hostname HOST_NAME
```

To create XL_MANAGER_PROFILE by using the Profile Management tool in the administrative console:

1. Select **Start**, **Programs**, **IBM WebSphere**, **Application Server Network Deployment**, and then select **Profile Management tool.**
2. Select **Deployment Manager**, and then click **Next**.
3. Select **Advanced Profile creation**, and then click **Next**.
4. Select **Deploy the administrative console**, and then click **Next**.
5. Enter `XL_MANAGER_PROFILE` for the Profile Name, change the profile directory to *`WEBSPHERE_HOME`*`\profiles\XL_MANAGER_PROFILE`, and then click **Next**.
6. Enter `XL_MANAGER_NODE` for the Node Name, `XL_CELL` for the Cell Name, and then click **Next**.
7. Clear the **Enable administrative security** option, and then click **Next**.
8. Click **Create** to create the profile.
9. On Port Values Assignment, click on the default Port values, and then click **Next**.

> **Note:** Make a note of the port numbers if you have selected the recommend ports.

10. On the Windows Service Definition window, deselect the Run the Deployment process as Windows service.

XL_MODEL_PROFILE for model node (XL_MODEL_NODE) on NDM_HOST

Create XL_MODEL_PROFILE by using the *`WEBSPHERE_HOME`*`/bin/manageprofiles` command on NDM_HOST, as shown:

For Microsoft Windows:

```
WEBSPHERE_HOME\bin\manageprofiles.bat -create
-templatePath "WEBSPHERE_HOME\profileTemplates\managed"
-profileName XL_MODEL_PROFILE -profilePath
"WEBSPHERE_HOME\profiles\XL_MODEL_PROFILE" -nodeName XL_MODEL_NODE
-hostname HOST_NAME
```

For UNIX:

```
WEBSPHERE_HOME/bin/manageprofiles.sh -create
-templatePath "WEBSPHERE_HOME/profileTemplates/managed"
-profileName XL_MODEL_PROFILE -profilePath
"WEBSPHERE_HOME/profiles/XL_MODEL_PROFILE" -nodeName XL_MODEL_NODE
-hostname HOST_NAME
```

To create XL_MODEL_PROFILE by using the Profile Management tool in the administrative console:

1. Select **Start**, **Programs**, **IBM WebSphere**, **Application Server Network Deployment**, and then select **Profile Management tool.**
2. Select **Custom Profile** for Environments and click **Next**.
3. Select **Advanced Profile creation**, and then click **Next**.
4. Enter `XL_MODEL_PROFILE` for the Profile Name, change the profile directory to *`WEBSPHERE_HOME`*`\profiles\XL_MODEL_PROFILE`, and then click **Next**.
5. Enter `XL_MODEL_NODE` for the Node Name, enter the name of the computer for the Hostname, and then click **Next**.

6. Select **Federate this node later**, and then click **Next**.
7. Click **Create** to create the profile.

XL_JMS_PROFILE for model node (XL_JMS_NODE) on JMS_HOST

Create XL_JMS_PROFILE by using the *WEBSPHERE_HOME*/bin/manageprofiles command on JMS_HOST, as shown:

For Microsoft Windows:

```
WEBSPHERE_HOME\bin\manageprofiles.bat -create
-templatePath "WEBSPHERE_HOME\profileTemplates\managed"
-profileName XL_JMS_PROFILE -profilePath "WEBSPHERE_HOME\profiles\XL_JMS_PROFILE"
-nodeName XL_JMS_NODE
-hostname HOST_NAME
```

For UNIX:

```
WEBSPHERE_HOME/bin/manageprofiles.sh -create
-templatePath "WEBSPHERE_HOME/profileTemplates/managed"
-profileName XL_JMS_PROFILE -profilePath "WEBSPHERE_HOME/profiles/XL_JMS_PROFILE"
-nodeName XL_JMS_NODE
-hostname HOST_NAME
```

To create XL_JMS_PROFILE by using the Profile Management tool in the administrative console:

1. Select **Start**, **Programs**, **IBM WebSphere**, **Application Server Network Deployment**, and then select **Profile Management tool.**
2. Select **Custom Profile** for Environments and click **Next**.
3. Select **Advanced Profile creation**, and then click **Next**.
4. Enter XL_JMS_PROFILE for the Profile Name, change the profile directory to *WEBSPHERE_HOME*\profiles\XL_JMS_PROFILE, and then click **Next**.
5. Enter XL_JMS_NODE for the Node Name, enter the name of the computer for the Hostname, and then click **Next**.
6. Select **Federate this node later**, and then click **Next**.
7. Click **Create** to create the profile.

XL_NODEn_PROFILE for XL_NODEn on NODEn_HOST

> **Note:** This profile must be created on each node host in the cluster that is running a WebSphere Application Server.
>
> For example, you can create XL_NODE1_PROFILE with node name XL_NODE1 on XL_NODE1_HOST computer and XL_NODE2_PROFILE with node name XL_NODE2 on XL_NODE2_HOST computer.
>
> The steps in this section apply only for XL_NODE1_PROFILE. To create rest of the profiles, replace the values appropriately.

Create XL_NODE1_PROFILE by using the *WEBSPHERE_HOME*/bin/manageprofiles command on XL_NODE1_HOST, as shown:

For Microsoft Windows:

```
WEBSPHERE_HOME\bin\manageprofiles.bat -create
-templatePath "WEBSPHERE_HOME\profileTemplates\managed"
-profileName XL_NODE1_PROFILE -profilePath
"WEBSPHERE_HOME\profiles\XL_NODE1_PROFILE" -nodeName XL_NODE1
-hostname HOST_NAME
```

For UNIX:

```
WEBSPHERE_HOME/bin/manageprofiles.sh -create
-templatePath "WEBSPHERE_HOME/profileTemplates/managed"
-profileName XL_NODE1_PROFILE -profilePath
"WEBSPHERE_HOME/profiles/XL_NODE1_PROFILE" -nodeName XL_NODE1
```

To create XL_NODE1_PROFILE by using the Profile Management tool in the administrative console:

1. Start the WebSphere administrative console.
2. Select **Custom Profile** for Environments and click **Next**.
3. Select **Advanced Profile creation**, and then click **Next**.
4. Enter `XL_NODE1` for the Profile Name, change the profile directory to *`WEBSPHERE_HOME`*`\profiles\XL_NODE1_PROFILE`, and then click **Next**.
5. Enter `XL_NODE1` for the Node Name, and then click **Next**.
6. Select **Federate this node later**, and then click **Next**.
7. Click **Create** to create the profile.

9.4.5 Setting JVM Memory and Arguments

For Oracle Identity Manager, JVM memory settings must be changed for production environments and/or when processing large volume in nonproduction.

Perform the following steps to set the JVM memory size. The WebSphere application server must be running to set the memory size.

To set the JVM memory size:

1. Connect to the WebSphere administrative console by using the following URL:

   `http://`*`WebSphere Host`*`:`*`WebSphere Admin Port`*`/admin`

   Note: The default WebSphere administrative console port is 9060.

2. Select **Servers**, and then select **Application Servers**.
3. Select the server name.
4. Go to Server Infrastructure, and then click **Java and Process Management.**
5. Select **Process Definition**.
6. Go to Additional Properties, and then click **Java Virtual Machine.**
7. Enter **1280** for Minimum Heap Size.
8. Enter **1280** for Maximum Heap Size.

9. Enter `-Xjit:disableLocalVP,disableGlobalVP` for Generic JVM arguments.
10. Click **OK**.
11. Click **Save** to commit the setting.

> **Note:** For clustered installation of WebSphere, these changes must be done for all the servers participating in the cluster.

9.4.6 Enabling SOAP Communication to WebSphere

The Oracle Identity Manager installer communicates with WebSphere as a SOAP client by using JACL commands to create data sources, set up message queues, and other operations. To enable SOAP, edit the following properties in the *WEBSPHERE_HOME*\profiles*PROFILE_NAME*\properties\soap.client.props file on all application servers in the cluster:

> **Note:** If you used a user ID or password other than xelsysadm for WebSphere, then enter the same user ID or password here.

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserid=xelsysadm
com.ibm.SOAP.loginPassword=xelsysadm_password
```

> **Note:** You must make this change for each newly created profile, for example, XL_MANAGER_PROFILE and XL_MODEL_PROFILE on the NDM_HOST computer, XL_NODEn_PROFILE on the XL_NODEn_HOST computer, and XL_JMS_PROFILE on the XL_JMS_NODE computer.

9.4.7 Verifying Installation

After you have installed and upgraded the WebSphere application server, perform the following steps to verify the installation:

1. Open the First Steps interface.

   From the **Start** menu, select **IBM WebSphere**, select a specific profile (**XL_MANAGER_PROFILE**), and then select **First Steps**.
2. Click **Verify Installation**.
3. After you have verified the installation, click **Stop the Server**.

9.4.8 Creating Backups

Back up the Nodes. Refer to the "Backing Up the Configurations" section on page 9-5 for more information about creating backups.

Back up the configurations of the following components:

- XL_MANAGER_NODE on NDM HOST
- XL_MODEL_NODE on NDM HOST
- Each XL_NODEn on XL_NODEn_HOST

- XL_JMS_NODE on XL_JMS_NODE

To create the backups for each node:

1. Create a backup directory for each node you have installed.

   For example, create the following:

   `C:\WAS_Backups\Basic\`*`Node`*`Config`

   Or:

   `/opt/WAS_Backups/Basic/`*`Node`*`Config`

2. Run the backup script from the *`WEBSPHERE_HOME`*`\profiles\`*`PROFILE_NAME`*`\bin` directory of the application server.
3. Zip the `installedApps` directory and save it in the same location.

9.5 Adding the Model Node to the Network Deployment Manager

After you have installed WebSphere and created profiles on the NDM_HOST, add the XL_MODEL_NODE to the Network Deployment Manager. To add a node, perform the following steps for each host computer:

1. Open a command prompt on NDM_HOST.
2. Change directories to the bin directory of XL_MODEL_PROFILE.

   Note: Before you perform Step 3, ensure that the Network Deployment Manager is running.

3. Run the addNode.bat or addNode.sh script, specifying the Network Deployment Manager host name.

   For example:

   `addNode.bat` *`NDM_HOST NDM_SOAP_PORT`*

   Where *`NDM_HOST`* is the host name of the Network Deployment Manager and *`NDM_SOAP_PORT`* is the SOAP port for the Network Deployment Manager.

   Note: Host name is case-sensitive.

To verify that the XL_MODEL_NODE is added:

1. Using a Web browser, connect to the administrative console by navigating to the following URL:

   `http://`*`NDM_HOST`*`:`*`NDM_PORT`*`/admin`

2. Log on to the system.
3. Click **System Administration**.
4. Click **Nodes**.

   If the nodes are added, then they are displayed with status as synchronized. You can see the status by rolling the mouse pointer over the icon displayed for the Node name in the Administrative and User Console.

5. Log out and then log in to the WebSphere administrative console to refresh the list of nodes.

9.6 Creating the Model Server

The model server serves as a template to create other servers for the cluster. The model server is not part of the cluster, and it does not serve any requests.

To create the model server:

1. Using a Web browser, connect to the Node Manager administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

2. Log on to the system.
3. Click **Servers** in the left panel.
4. Click **Application Servers**.
5. Click **New**.
   a. Select the model node (XL_MODEL_NODE).
   b. Enter **XL_MODEL_SERVER** as the server name, and then click **Next**.
   c. Select the second option for the default application server template, and then click **Next**.
   d. Ensure that the **Generate Unique Ports** option is selected.
   e. Click **Next**.
6. Click **Finish**.

   XL_MODEL_SERVER is displayed in the list of application servers.
7. Select **Preferences, Synchronize changes with Nodes**, and then click **Apply**.
8. Click **Save** to commit your changes.

Note: Your changes are not saved until you click **Save**.

9.7 Creating the XL_CLUSTER

A cluster is a group of application servers that appear as one to the clients. All application servers that are used to service incoming calls must be part of this cluster. After you create the empty cluster, back up the system.

To create the cluster:

1. Using a Web browser, connect to the Network Deployment Manager administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

2. Log on to the system.
3. Click **Servers** in the left panel.
4. Click **Clusters**.
5. Click **New**.

- Enter **XL_CLUSTER** as the cluster name.
- Ensure that you select the **Prefer local** and **Configure HttpSession memory-to-memory replication** check boxes, and then click **Next**.

6. Ensure that the **None, Create an empty cluster** option is selected, and then click **Next**.
7. Click **Finish**.
8. Select **Preferences, Synchronize changes with Nodes**, and then click **Apply.**
9. Click **Save**.

   The XL_CLUSTER is created. At this point, it is an empty cluster.

> **Note:** You must click **Save** to save the changes you made.

9.8 Creating the JMS CLUSTER

JMS cluster is used to manage JMS messages. After you create the empty cluster, ensure that you back up the system.

To create the JMS cluster:

1. Using a Web browser, connect to the Network Deployment Manager administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

2. Log on to the system.
3. Click **Servers** on the left panel.
4. Click **Clusters**.
5. Click **New**.
   - Enter **XL_JMS_CLUSTER** as the cluster name.
   - Ensure that you select the **Prefer local** and **Configure HttpSession memory-to-memory replication** options.
6. Ensure that the **None, Create an empty cluster** option is selected, and then click **Next**.
7. Click **Finish**.
8. Select **Preferences, Synchronize changes with Nodes**, and then click **Apply.**
9. Click **Save**.

   The XL_JMS_CLUSTER is created. At this point, it is an empty cluster.

> **Note:** You must click **Save** to save the changes you made.

9.9 Backing Up the Nodes

Back up the Nodes. Refer to the "Backing Up the Configurations" section on page 9-5 for more information about creating backups.

Back up the configurations of the following components:

- XL_MANGER_NODE on NDM_HOST

- XL_MODEL_NODE on NDM_HOST

To create the backups for each node:

1. Create the backup directories:

   `C:\WAS_Backups\PreXL\`*`Node`*`Config`

   Or:

   `/opt/WAS_Backups/PreXL/`*`Node`*`Config`

   `Node` represents the name of the component.

2. Run the backup script from the bin directory on the application server.
3. Zip the `installedApps` directory and save it in the same location.

The configuration backup command stops the Network Deployment Manager and all the nodes that it runs on. While it is possible to get backups without stopping the nodes or Network Deployment Manager, Oracle recommends that you stop them before getting the configuration backups. After completing the configuration backups, ensure that you restart the Network Deployment Manager (use startmanager.bat or startmanager.sh) as well as the Nodes (use startnode.bat or startnode.sh).

9.10 Installing and Configuring a Database for Oracle Identity Manager

Refer to Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager" for information.

9.11 Installing Oracle Identity Manager on the Network Deployment Manager

In a WebSphere cluster, install Oracle Identity Manager on the Node Manager. From that installation, deploy Oracle Identity Manager to the application servers in the cluster. Because the Oracle Identity Manager installer communicates with the Node Manager server during the installation, ensure that the deployment manager is running.

Note: Stop all other applications running on the NDM_HOST, except for the Node Manager on XL_MANAGER_NODE and the Model Node XL_MODEL_NODE.

To install the Oracle Identity Manager on the Node Manager on Microsoft Windows:

1. Double-click the **setup_server.exe** file, and then click **Next**.
2. Select a language on the Installer page and click **OK**. The Welcome page is displayed.
3. Click **Next** on the Welcome page. The Admin User Information page is displayed.
4. Enter a password you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then click **Next**. The OIM Application Options page is displayed.
5. Select **Oracle Identity Manager** or **Oracle Identity Manager with Audit and Compliance Module**, and then click **Next**.

6. Select the destination directory to install Oracle Identity Manager, and then click **OK**.
7. Click **Next**.
8. Click **Next**.
9. Select the database type, and then click **Next**.
10. Enter the database information, and then click **Next**.
11. Select the authentication, and then click **Next**.
12. Select **IBM WebSphere** and click **Next**.
13. Select **Yes** for clustering.
14. Enter the cluster name, and then click **Next**.
15. Enter the Network Deployment Manager Information.
    a. Provide the location in which the Deployment Manager is installed. The default path is `C:\Program Files\IBM\WebSphere\AppServer`.
    b. Provide the location of the Deployment Manager's JDK. The default path is `C:\Program Files\IBM\WebSphere\AppServer\java`.
    c. Click **Next**.
16. For the WebSphere information.
    a. Provide the host name of the computer running the Deployment Manager (NDM-HOST).

       Note: Do not use localhost. Specify the host name or IP address.

    b. Enter the cell name (XL_CELL).
    c. Enter the model node name (XL_MODEL_NODE).
    d. Enter the model server name (XL_MODEL_SERVER).
    e. Enter the profile name (XL_MANAGER_PROFILE)
    f. Click **Next**.
17. Enter the JMS cluster name (XL_JMS_CLUSTER).
18. Click **Next**, and then click **Install** to install Oracle Identity Manager.

    This might take some time. Watch the SystemOut.log file in the *WEBSPHERE_HOME*`\profiles\XL_MANAGER_PROFILE\logs\dmgr\` directory to monitor the progress.
19. Click **Finish** to complete the installation.

To install the Oracle Identity Manager on the Node Manager on UNIX or Linux:

1. From the console, go to the `installServer` directory on the installation CD and run the install_server.sh by using the following command:

   ```
   sh install_server.sh
   ```

> **Note:** If you are not installing Oracle Identity Manager from distributed media (a CD), then you must set the execute bit of all shell scripts in the installServer directory. To set the execute bit for all shell scripts recursively, go to the installServer directory and run the `chmod -R u+x *.sh` command.

The installer starts in console mode.

2. Choose a language by entering a number from the list of languages.

   Enter **0** to apply the language selection. The Welcome Message panel is displayed.

3. Enter **1** on the Welcome Message panel to display the next panel.

   The Admin User Information panel is displayed.

4. Enter a password you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then enter **1** to move to the next panel.

   The OIM Application Options panel is displayed.

5. Enter **1** on the OIM Application Options panel to display the next panel.

   The Select the Oracle Identity Manager application to install panel is displayed.

6. Select the application to install:

   – Enter **1** for Oracle Identity Manager.

   – Enter **2** for the Oracle Identity Manager with Audit and Compliance Module.

   After selecting the application, enter **0**, and then enter **1** to move to the next section. The Target directory panel is displayed.

7. In the Target directory panel, complete one of the following steps:

   - Enter the path to the directory in which you want to install Oracle Identity Manager, for example, `/opt/oracle/`.
   - Enter **1** to move to the next panel.

   If the directory does not exist, you are asked to create it. Enter **y**, for yes. The Database Server Selection panel is displayed.

8. Specify the type of database you are using.

   - Enter **1** to select Oracle.
   - Enter **2** to select SQL Server.
   - Enter **0** to finish.
   - Enter **1** to move to the next panel.

   The Database Information panel is displayed.

9. Enter your database information:

   a. Enter the database host name or IP address.

   b. Enter (or accept the default) port number.

   c. Enter the SID for the database name.

   d. Enter the database user name for the account that Oracle Identity Manager uses to connect to the database.

e. Enter the password for the database account that Oracle Identity Manager uses to connect to the database.

f. Enter **1** to move to the next panel.

The Authentication Information panel is displayed.

10. Select the authentication mode for the Oracle Identity Manager Web application.
    - Enter **1** for Oracle Identity Manager Default Authentication.
    - Enter **2** for SSO Authentication.
    - Enter **0** when you are finished.
    - If you select SSO authentication, then you must provide the header variable used in the Single Sign-On system when prompted.
    - Enter **1** to move to the next panel.

    The Application Server Selection panel is displayed.
11. Specify your application server type.
    - Enter **2** for IBM WebSphere.
    - Enter **0** when you are finished.
    - Enter **1** to move to the next panel.

    The Cluster Information panel is displayed.
12. On the Cluster Information panel:
    - Enter **1** for Yes.
    - Enter **0** when you are finished.
    - Enter the cluster name at the prompt.
    - Enter **1** to move to the next section.

    The Application Server Information panel is displayed.
13. Enter the Network Deployment Manager Information.
    a. Provide the location in which the Deployment Manager is installed. The default value is `/opt/IBM/WebSphere/AppServer`.
    b. Provide the location of the Deployment Manager's JDK. The default value is `/opt/IBM/WebSphere/AppServer/java`.
    c. Enter **1** to move to the next section.
14. For the WebSphere information:
    a. Provide the host name of the computer running the Deployment Manager (NDM_HOST).

    Note: Do not use localhost. Specify the host name or IP address.

    b. Enter the cell name (XL_CELL).
    c. Enter the model node name (XL_MODEL_NODE).
    d. Enter the model server name (XL_MODEL_SERVER).
    e. Enter the profile name (XL_MANAGER_PROFILE).

f. Enter **1** to move to the next section.

15. Enter the JMS cluster name (XL_JMS_CLUSTER) in JMS page.
16. When a message is displayed warning you to back up the application server, proceed to back up your installation, then enter **1** to move to the next section.
17. In the Installation summary information page, verify the information displayed, then do one of the following:
    - Enter **2** to go back and make changes.
    - Enter **1** to start the installation.
18. After Oracle Identity Manager installs, the Completed panel is displayed. Enter **3** to finish and exit.

9.11.1 Verifying the Installation

After successful installation, the Oracle Identity Manager application is visible on the Deployment Manager administrative console.

To verify the installation:

1. Using a Web browser, connect to the Node Manager administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

   Note: If you are using an administrative console browser window that you had logged on to before the Oracle Identity Manager installation, then log out and log back again to refresh the display.

2. Log on to the system.
3. Click **Applications** on the left panel.
4. Click **Enterprise Applications**.

   Xellerate and Nexaweb are displayed in the list of applications.

9.12 Backing up Configuration Settings

Back up the configurations for the following components:

- XL_MANAGER_NODE (under XL_MANAGER_PROFILE)
- XL_MODEL_NODE (under XL_MODEL_NODE)

To create the backups for each node:

1. Create the backup directories, for example:

   `C:\WAS_Backups\PostXL\NodeConfig`

   Or:

   `/opt/WAS_Backups/PostXL/NodeConfig`

2. Run the backup script from the bin directory of the application server or Node Manager.
3. Zip the `installedApps` directory, then save it in the same location.

4. Restart the Node Manager and the Nodes.

The backup command stops the node manager and the node agents on their respective computers. All these nodes and the node manager must be restarted to continue with the installation.

To restart the node manager on NDM_HOST:

1. Change to the bin directory. For example:

```
cd C:\Program Files\WebSphere\AppServer\profiles\XL_MANAGER_PROFILE\bin
```

2. Run the start command and specify the user and password.

   For example:

```
startmanager.bat -username xelsysadm -password Xelsysadm_Password
```

Note:

- If you use a user ID or password other than xelsysadm, then enter the same user ID or password here.
- From this point on, you must specify the proper user name and password to start or stop the Node Manager or the nodes in this cell. This is the result of Oracle Identity Manager setting up the WebSphere custom registry for JAAS authentication.

To restart a node on the node host:

1. Change to the bin directory. For example:

```
cd WEBSPHERE_HOME\profiles\XL_MODEL_PROFILE\bin
```

2. Run the start command and specify the user and password. For example:

```
startnode.bat -username xelsysadm -password Xelsysadm_Password
```

9.13 Adding Nodes to WebSphere Cell

WebSphere cell XL_CELL now contains only XL_MANAGER_NODE and XL_MODEL_NODE. When you installed WebSphere on other computers, such as XL_NODE1_HOST, XL_NODE2_HOST,… XL_NODEnHOST, and XL_JMS_HOST, each node was named appropriately, such as XL_NODE1, XL_NODE2, … XL_NODEn, and XL_JMS_NODE. For adding cluster members, you have to add all these nodes to the cell XL_CELL.

Before you can add a node, you need the SOAP port number that NDM uses to listen for and service administrative commands.

To get the SOAP port:

1. Ensure that Node Manager is running.
2. Using a Web browser, connect to the Node Manager administrative console by navigating to the following URL:

```
http://NDM_HOST:NDM_PORT/admin
```

3. Log in using Oracle Identity Manager Administrator name and password you specified during installation.
4. Click **System Administration** in the left panel.
5. Click **DeploymentManager**.
6. Click **Ports**.
7. Make a note of the port number for **SOAP_CONNECTOR_ADDRESS**.

   This port number is needed to add a node to the cell.

> **Note:** You also need this port number to update the JNDI references. Refer to the "Updating the JNDI References" section on page 9-26 for more information.

To finish setting up the cluster, for each node:

1. Ensure that the name and path of the *JAVA_HOME* directory used by Oracle Identity Manager is the same across all the nodes of the cluster.
2. Copy the *OIM_HOME* directory from NDM_HOST to the node host.

   Ensure that you copy it to the same location, such as, `C:\oracle`.
3. On the node host, change directories and move to the Oracle Identity Manager setup directory. For example, use the following command:

   ```
   cd C:\oracle\xellerate\setup
   ```
4. Open the xlAddNode.cmd or xlAddNode.sh script and set the path to the WebSphere installation directory on the node host.
5. Run the xlAddNode.cmd or xlAddNode.sh script under *OIM_HOME*`/setup/` directory. This script adds the node to the NDM, sets up the custom registry, sets the system properties, synchronizes the node with the NDM, and starts the node. Run the script with the following parameters:

   For Microsoft Windows:

   ```
   xlAddNode.cmd NODE_PROFILE_NAME NODE_NAME NDM_HOST NDM_SOAP_PORT user password
   ```

   For UNIX:

   ```
   xlAddNode.sh NODE_PROFILE_NAME NODE_NAME NDM_HOST NDM_SOAP_PORT user password
   ```

   For example, to add XL_NODE1, use the following command:

   ```
   xlAddNode.cmd XL_NODE1_PROFILE XL_NODE1 NDM_HOST 8879 xelsysadm
   xelsysadm_password
   ```

> **Notes:**
>
> - You must run the command for each node that you create.
>
>   If you used a user ID or password other than xelsysadm, then enter the same used ID or password here.
> - Node names are case-sensitive.

6. Create one or more servers on each node, such as XL_NODE1, XL_NODE2, … XL_NODEn.

   Refer to the "Creating Servers for XL_CLUSTER" section on page 9-23 for more information.

7. Create two servers for JMS on XL_JMS_NODE.

   Refer to the "Creating Servers for XL_JMS_CLUSTER" section on page 9-24 for more information.

8. Set up virtual host information for each server.

   Refer to the "Setting up the Server Virtual Host Information" section on page 9-25 for more information.

9.13.1 Creating Servers for XL_CLUSTER

Create one or more servers on each node, such as XL_NODE1, XL_NODE2, … XL_NODEn, which are members of the XL_CLUSTER. Use the Node Manager administrative console to do this.

To create a server:

1. Ensure that NDM is running.
2. Using a Web browser, connect to the NDM administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

3. Log in by using Oracle Identity Manager Administrator name and password that you specified during installation.
4. Click **Servers**.
5. Click **Clusters**.
6. Click **XL_CLUSTER**.
7. Go to Additional Properties, and then click **Cluster members**.
8. Click **New**, and then:
   a. Name the server. Use a descriptive naming convention for the cluster member name, such as XL_SERVER1_ON_NODE1.
   b. Select the node to manage this server (XL_NODE1).
   c. Select the second option of **creating using an existing application server as a template**.
   d. Select **XL_CELL/XL_MODEL_NODE/XL_MODEL_SERVER** and click **Next**.
   e. Add additional members for the other existing nodes by using Add Members and by entering the succeeding set of information, for example, XL_SERVER2_ON_NODE2 as server name and XL_NODE2 as the node name.

      Similarly create all servers and add to the cluster.

   f. Click **Add Member**.
9. Click **Next**.
10. Click **Finish**.
11. Select **Preferences**, Synchronize changes with Nodes, and then click **Apply.**

12. Click **Save**.

    The servers are created as members of the XL_CLUSTER.

9.14 Creating Servers for XL_JMS_CLUSTER

Create at least two servers that are members of the XL_JMS_CLUSTER for better failover capabilities. Use the Node Manager administrative console to do this.

To create servers for XL_JMS_CLUSTER:

1. Ensure that NDM is running.
2. Using a Web browser, connect to the NDM administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

3. Log in by using Oracle Identity Manager Administrator name and password that you specified during installation.
4. In the left panel, click **Servers**.
5. Click **Clusters**.
6. Click **XL_JMS_CLUSTER**.
7. Go to Additional Properties, and then click **Cluster members**.
8. Click **New**, and then:
   a. Name the server. Use a descriptive naming convention for the cluster member name, such as XL_JMS_SERVER1.
   b. Select the node to manage this server (XL_JMS_NODE).
   c. Select the second option of **creating using an existing application server as a template**.
   d. Select **XL_CELL/XL_MODEL_NODE/XL_MODEL_SERVER** and click **Next**.
   e. Add additional members for the other existing nodes by using Add Members (add XL_JMS_SERVER2).
   f. Click **Add Member**.
9. Click **Next**.
10. Click **Finish**.
11. Select **Preferences, Synchronize changes with Nodes,** and then click **Apply.**
12. Click **Save**.

    The servers XL_JMS_SERVER1 and XL_JMS_SERVER2 are created as members of XL_JMS_CLUSTER.

9.14.1 Enabling SIB Services for XL_JMS_CLUSTER Servers

To enable SIB services for XL_JMS_CLUSTER servers:

1. Ensure that NDM is running.
2. Using a Web browser, connect to the NDM administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

3. Log in by using Oracle Identity Manager Administrator name and password that you specified during installation.
4. In the left panel, click **Servers**.
5. Click **Application Servers**.
6. Click **XL_JMS_SERVER1**.
7. Go to Server Messaging, and click **SIB service**.
8. In General Properties, check **Enable service at startup.**
9. Click **OK.**
10. Click **Preferences**, and then select **Synchronize changes with Nodes.**
11. Click **Save.**

Repeat the procedure for all servers in the XL_JMS_CLUSTER, for example XL_JMS_SERVER1 and XL_JMS_SERVER2.

9.15 Setting up the Server Virtual Host Information

The application server uses the virtual host information setup on the Node Manager to properly configure the Web server plug-ins to distribute the load and deal with failover. When you add a server to the cluster, update the virtual host information.

To update the virtual host information:

1. Ensure that Node Manager is running.
2. Using a Web browser, connect to the Node Manager administrative console by navigating to the following URL:

   `http://NDM_HOST:NDM_PORT/admin`

3. Log in by using Oracle Identity Manager Administrator name and password that you specified during installation.
4. In the left panel, click **Servers**.
5. Click **Application Servers**.
6. Click **XL_SERVER1_ON_NODE1**.
7. In the Communications section, click **Ports.**
8. Note the port numbers shown on this page for WC_defaulthost and WC_defaulthost_secure, for example, port 9081 for WC_defaulthost and 9444 for WC_defaulthost_secure.
9. In the left panel, click **Environment**.
10. Click **Virtual Hosts**.
11. Click **default_host**.
12. Click **Host Aliases**.
13. Click **New**, and then:
    a. Enter * for the Host Name.
    b. In the **Port** field, enter the previously noted WC_defaulthost port number.
14. Click **Apply**.

15. At the top of this page, click **Host Aliases**.
16. Click **New**, and then:
    a. Enter * for the **Host Name**.
    b. In the **Port** field, enter the previously noted WC_defaulthost_secure port number.
17. Click **Apply**.
18. Select **Preferences, Synchronize changes with Nodes,** and then click **Apply.**
19. Click **Save**.

Virtual host setup for the XL_SERVER1_ON_NODE1 server is complete.

Repeat the procedure for all available servers in XL_CLUSTER, for example, XL_SERVER1_ON_NODE2.

9.16 Updating the JNDI References

When cluster members are added or removed, the JNDI references in Oracle Identity Manager must be updated. The JNDI references include the host name and WebSphere bootstrap port numbers for each server in the cluster. The JNDI references are specified in the xlconfig.xml file in Oracle Identity Manager.

Oracle provides a tool that communicates with the Node Manager, gets the list of servers that are part of the cluster with the corresponding bootstrap ports, constructs the JNDI URL, and prints it out. Update the xlconfig.xml file on each of the nodes with this URL.

To update the JNDI reference:

1. On NDM_HOST, change to the Oracle Identity Manager setup directory.

   For example, use the command:

   ```
   cd C:\oracle\xelleate\setup
   ```

2. Edit the `webspherеConfigUtility.cmd` or `webspherеConfigUtility.sh` script to ensure that the values of the `WS_HOME` and `XL.HomeDir variables` are set correctly.
3. Run the command file.

   For example, use the following command with arguments.

   ```
   webspherеConfigUtility.cmd NDM_HOST SOAP_PORT
   xelsysadm xelsysadm_password getjndiurl
   ```

   Note: If you used a user ID or password other than xelsysadm for WebSphere, then enter the same user ID or password here.

   See Also: The "Adding Nodes to WebSphere Cell" section on page 9-21 for information about getting the SOAP_PORT number

   The output from the tool includes a JNDI URL. For example:

   ```
   corbaloc:iiop:XL_NODE1_HOST:9812,XL_NODE2_HOST:9813
   ```

Note: This sample URL includes references to two cluster members (servers).

4. Edit the `xlconfig.xml` file in the *`OIM_HOME`*`\config` directory.

   Replace all four instances of the java.naming.provider.url with the URL from the tool.

   Note: Use the URL for the Design Console also. Refer to the "Installing Oracle Identity Manager Cluster By Using a Shared Directory" section on page 9-31 for more information.

5. Save and close the xlconfig.xml file.
6. Copy the modified xlconfig.xml file to all the nodes in XL_CELL, that is, to the corresponding *`OIM_HOME`*`\config` directory to all the hosts such as XL_JMS_HOST, XL_NODE1_HOST, XL_NODE2_HOST, and so on.
7. After you copy this file to all the nodes, restart the servers in the XL_CLUSTER.

   Use the Node Manager administrative console to do this. Ensure that Node Manager is running.
8. Using a Web browser, connect to the Node Manager administrative console by navigating to the following URL:

   `http://`*`NDM_HOST`*`:`*`NDM_PORT`*`/admin`
9. Log in by using Oracle Identity Manager Administrator name and password that you specified during installation.
10. In the left panel, click **Servers**.
11. Click **Application Servers**.
12. Ensure that the options for all the Oracle Identity Manager servers (<XL_SERVERn_ON_NODEn>) are selected.

    These are the servers that run the Oracle Identity Manager application.

    Note: Ensure that the JMS servers are running before you start the XL_SERVER nodes.

13. Click **Start**.

    After the servers start, the green arrow in the status column indicates that the servers are running.

9.17 Setting Up IIS as Web server

The following steps describe the high-level tasks associated with installing IIS as Web server, installing WebSphere plug-in for IIS, and its related configuration tasks:

- Installing IIS
- Installing the WebSphere Plug-in for IIS
- Configuring the IIS Plug-in

9.17.1 Installing IIS

The front end for WebSphere cluster is an IIS server running on *IIS_HOST*. Clients connect to this IIS Web server that sends requests to the WebSphere servers in the XL_CLUSTER cluster.

To verify that IIS is installed:

1. On *IIS_HOST*, open the **Control Panel** and select **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select **Application Server**, and then click **Details**.
4. If IIS is not installed, then select **Internet Information Service (IIS)**.
5. Click **Next**. IIS installs.
6. Click **Finish**.

9.17.2 Installing the WebSphere Plug-in for IIS

The WebSphere plug-in is installed by performing a custom WebSphere installation on *IIS_Host*.

To install the plug-in on Microsoft Windows 2000:

1. Start the installation wizard for the Web Server plug-ins.
2. Select the **Microsoft Internet Information Services** option.
3. Select **Webserver machine (remote)** option.
4. Provide the path for the installation.
5. Specify the port (default value is `80`).
6. Specify the Web server name (default name is `webserver1`).
7. Accept the location of default `plugin-cfg.xml` file and continue.
8. Specify the IP address of the application server.
9. To enable the plug-in within IIS, and then verify that it is working, start the Internet Services Manager in Administrative Tools.
10. Right-click the icon for the IIS server, and then select **Restart IIS** from the shortcut menu.
11. Click **OK** to restart the IIS Service, and enable the WebSphere plug-in for IIS.
12. After the restart process finishes, right-click the server, and then select **Properties** from the shortcut menu.
13. Click **Edit** beside **WWW Services** under Master Properties.
14. In the ISAPI Filters tab, ensure that **sePlugins** is displayed with high priority indicated by a green upward arrow. If **sePlugins** is not displayed in the ISAPIFilters tab, then:
    a. Click **Add**. Use **sePlugins** as FilterName, and specify *PLUGIN_HOME*`/bin/`*IIS_webserver_name*`/iisWASPlugin_http.dll` as the executable file.
    b. Click **OK** to add the filter.
    c. Restart IIS Service and check the property of the DefaultWebSite again. Priority of the ISAPIFilter might still be Unknown. It would take time

(possibly hours or even a day) for it to be updated as high priority with the green upward arrow.

To install the plug-in on Microsoft Windows 2003:

1. Start the installation wizard for the Web Server plug-ins.
2. Select the **Microsoft Internet Information Services** option.
3. Select **Webserver machine (remote)** option.
4. Provide the path for the installation.
5. Specify the port (default value is `80`).
6. Specify the Web server name (default name is `webserver1`).
7. Accept the location of default `plugin-cfg.xml` file and continue.
8. Specify the IP address of the application server.
9. To enable the plug-in within IIS, and then verify that it is working, start the Internet Information Services (IIS) Manager in Administrative Tools.
10. Expand the computer name.
11. Expand the **Web Sites** folder.
12. Right-click **Default Web Site**, select **New**, and then click **Virtual Directory**.
13. In the Welcome to Virtual Directory Creation Wizard window, click **Next** to go to the next window.
14. In the Virtual Directory Alias window, enter `sePlugins` as the alias, and then click **Next**.
15. In the Web Site Content Directory window, browse to the location where you install the WebSphere Plug-ins. Ensure that you include the `bin` directory, for example, `C:\WSPlugin\bin`, and then click **Next**.
16. In Virtual Directory Access Permissions, ensure that the **Read**, the **Run Scripts**, and the **Execute** options are selected. Click **Next** after you finish selecting the permissions.
17. Click **Finish**.
18. Right-click the computer icon, select **All Tasks**, and then click **Restart IIS**.
19. Click **OK** to restart the IIS Service and enable the WebSphere plug-in for IIS.
20. After the restart process finishes, expand the **Web Site** folder, right-click **Default Web** Site, and then select **Properties** from the shortcut menu.
21. In the ISAPI Filters tab, ensure that **sePlugins** is displayed with high priority and is indicated by a green upward arrow. If **sePlugins** is not displayed in the ISAPIFilters tab, then:
    a. Click **Add**. Use **sePlugins** as FilterName, and specify *`PLUGIN_HOME`*`/bin/`*`IIS_webserver_name`*`/iisWASPlugin_http.dll` as the executable file.
    b. Click **OK** to add the filter.
    c. Restart IIS Service and check the property of the DefaultWebSite again. Priority of the ISAPIFilter might still be Unknown. It would take time (possibly hours or even a day) for it to be updated as high priority with the green upward arrow.

9.17.3 Configuring the IIS Plug-in

This section discusses how to configure the IIS plug-in, export the configuration from the Node Manager, and install it.

To configure the IIS plug-in and install the configuration:

1. Ensure that Network Deployment Manager (NDM) is running.
2. Copy configurewebserver1.bat (for Windows) or configurewebserver1.sh (for UNIX) from *IIS_HOST* computer to the following directory on *NDM_HOST*:

   WEBSPHERE_HOME/profiles/XL_MANAGER_PROFILE/bin/

   Note: configurewebserver1.bat is located in the following directory on *IIS_HOST*:

   PLUGIN_HOME/bin

   configurewebserver1.sh is located in the following directory:

   PLUGIN_HOME/bin/crossPlatformScripts/unix

3. Run the configurewebserver1 script to generate the IIS plugin file on *NDM_HOST*.
   - For Windows *NDM_HOST*: Configurewebserver1.bat -profileName XL_MANAGER_PROFILE -user xelsysadm -password *xelsyadm_password*
   - For UNIX *NDM_HOST*: Configurewebserver1.sh -profileName XL_MANAGER_PROFILE -user xelsysadm -password *xelsyadm_password*

   Note: For cross-platform configurations (IIS Web server on Windows and WebSphere server on UNIX), changes are required to compensate for file encoding differences to prevent the Configurewebserver1.sh script from failing.

   For more information, visit:
   http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tins_webplugins_remotesa.html

4. Search for plugin-cfg.xml under the *WEBSPHERE_HOME*/profiles/XL_MANAGER_PROFILE/ directory. There are two plugin-cfg.xml files. Choose the one that is *not* *WEBSPHERE_HOME*/profiles/XL_MANAGER_PROFILE/config/cells/plugin-cfg.xml.
5. Copy the new plugin-cfg.xml file from the Network Deployment Manager to the install directory of the IIS server WebSphere plug-in.
6. Open the file on the IIS server. Several paths in the new configuration file must be updated to reflect the files of the IIS server.
7. Save and close the file.
8. Restart the IIS server.

9.18 Installing Oracle Identity Manager Cluster By Using a Shared Directory

Use the following task overview to install Oracle Identity Manager on a WebSphere clustered environment by using a shared directory. You must perform the steps in the task overview in the order shown.

To install Oracle Identity Manager cluster by using a shared directory:

1. Create a shared directory on the file server designated for Oracle Identity Manager.

   This shared directory can be on a Solaris computer with NFS or on a Microsoft Windows share.

2. On all the computers that will be hosting Oracle Identity Manager, map this drive by using the same drive letter on each computer.

   If the installation is on Solaris, then mount the NFS partition on the same mount point.

3. Install Oracle Identity Manager by using the standard installation instructions.

   Provide the installation location on the shared drive.

4. When adding a new host to the cluster, map the drive as in step 2, thereby making Oracle Identity Manager home directory available for use.

5. Modify the xlAddNode command to provide the proper Oracle Identity Manager location as well as the WebSphere location.

6. Run the xlAddNode command.

Note: If the log.properties file is modified to include a File Appender to log the Oracle Identity Manager messages into a separate file, then ensure that you provide a location on the local drive. Also, ensure that the same location exists on all the nodes.

9.19 Partitioned Installation on WebSphere

This section describes how to perform a partitioned installation of Oracle Identity Manager in a WebSphere clustered environment.

WebSphere clustered environments for a partitioned installation are the following:

- An **independent clustered environment** in which Scheduled Task and Front Office are processed

  Two independent installations of Oracle Identity Manager share the same database.

- A **multiple clustered environment** in which the same Network Deployment Manager (NDM) is used for hosting different components.

9.19.1 Important Points to Consider

Here are some important points to consider before you choose the type of clustered environment you wish to install the partitioned Oracle Identity Manager:

- Adapters and scheduled jobs can invoke APIs and submit messages.

These API calls are processed in which APIs are hosted at the Core Server. Also, the submitted messages are processed in which Message Driven Beans (MDBs) are hosted. Therefore, scheduled job execution is truly distributed among three components: the APIs, the MDBs and the Schedule Job itself.

- All off-lined tasks will be executed partly by the API layer and partly by the MDB layer.

  Currently, request initiation and reconciliation are off-lined, but more tasks are planned to be off-lined in the future.

- In theory, it is possible to install a Scheduler a single computer.

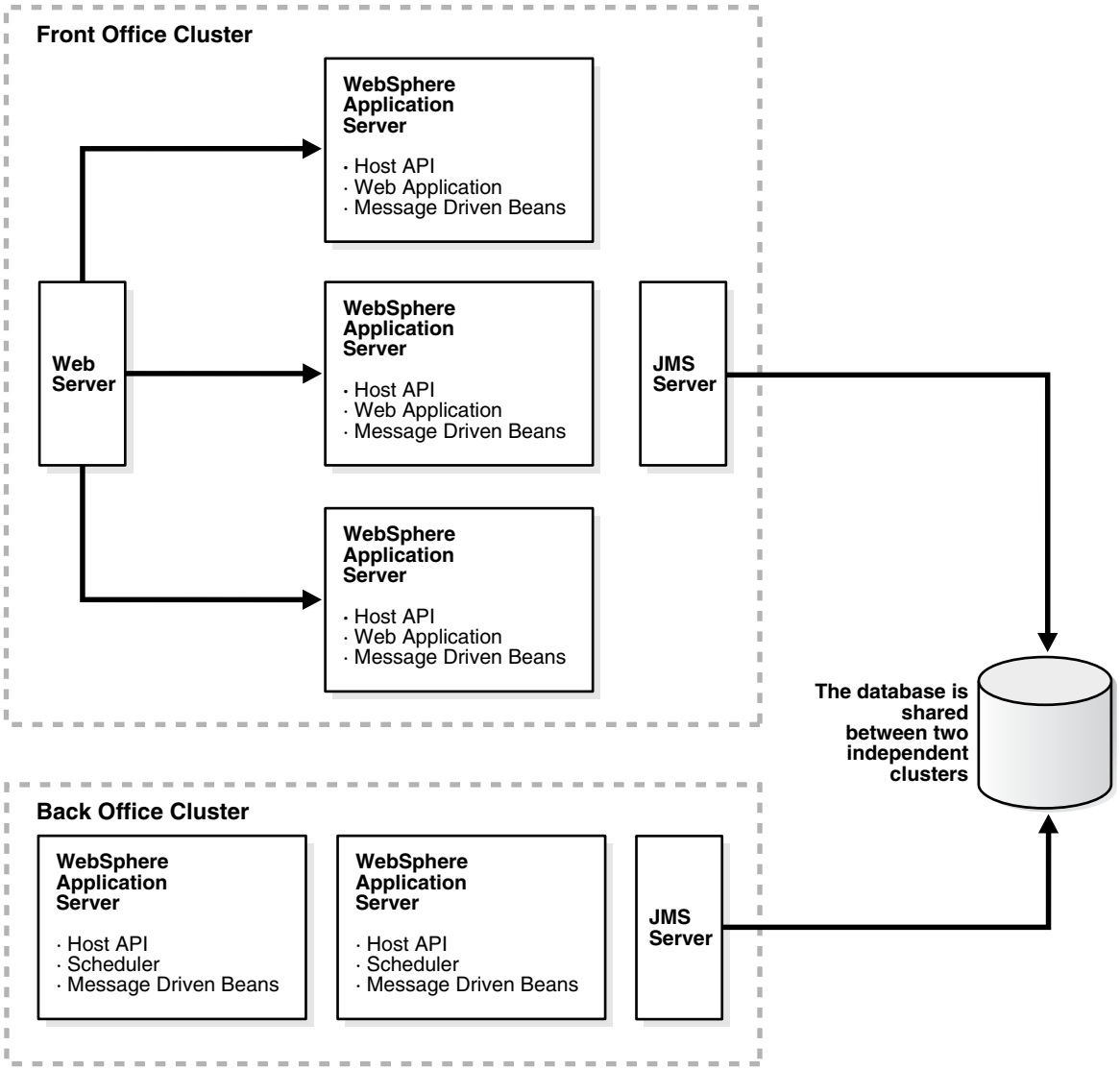
  However, when a schedule task runs, it calls the APIs. For the reconciliation tasks, they call APIs as well as submit messages. Therefore, true processing of scheduled tasks occurs in the APIs and MDBs.

9.20 Independent Clustered Installation

For an independent clustered environment, two separate Oracle Identity Manager installations share the same database. The first installation of Oracle Identity Manager is designed to handle Front Office, which is the user requests for administration, provisioning, and so on. The second installation is designed to handle Back Office for only the Schedule Task execution.

Figure 9–2 shows two independent clustered environments: Front Office and Back Office.

Figure 9–2 Two Independent Oracle Identity Manager Cluster Environments



9.20.1 Environment Profile

The following items discuss some important points needed for the independent clustered environment:

- The Front Office installation must include MDBs because the Front Office is not aware of the existence of the Back Office.

  However, it is possible to overcome this limitation by using WebSphere MQ.

- The Back Office installation must include APIs because they are called by the Scheduled Tasks.

- Both installations can be either clustered or nonclustered.

  For example, Front Office can be a cluster, while Back Office runs on a single but powerful computer.

- Caching must be configured as a single cluster by using the same multi-cast IP address between both the clusters.

- If the same IP cannot be used, then the cache must be flushed in both the clusters after an import or a change to process definition, resource object definition, and so on.

9.20.2 Environment Advantages

Independent clustered environment has the following advantages:

- The clustered environments use different platform types.

  For example, the Front Office can be Windows-based, while the Back Office is Solaris-based.

- The entire Schedule Task execution is processed in the Back Office cluster with reasonable predictability.
- There is one Java Virtual Machine (JVM) for each computer, or one application server instance running for each computer.

Note: Ensure that the Cache\MultiCastAddress is same for both the Front Office and Back Office installations to ensure cache flushing on both clusters.

9.20.3 Environment Disadvantages

Independent clustered environment has the following disadvantages:

- The clusters are rigid in their processing duties.

  For example, the Front Office processing cannot be delegated to the Back Office cluster, and vice-versa even if the other cluster is under-utilized at that time. Therefore, under no circumstances can the Front Office cluster share the load on the Back Office cluster.

- The Design Console must be configured to work with the Back Office cluster and be able to schedule jobs, and so on.
- Because the Back Office cluster does not qualify as a true back-office cluster, it causes the limitation of off-lined tasks.

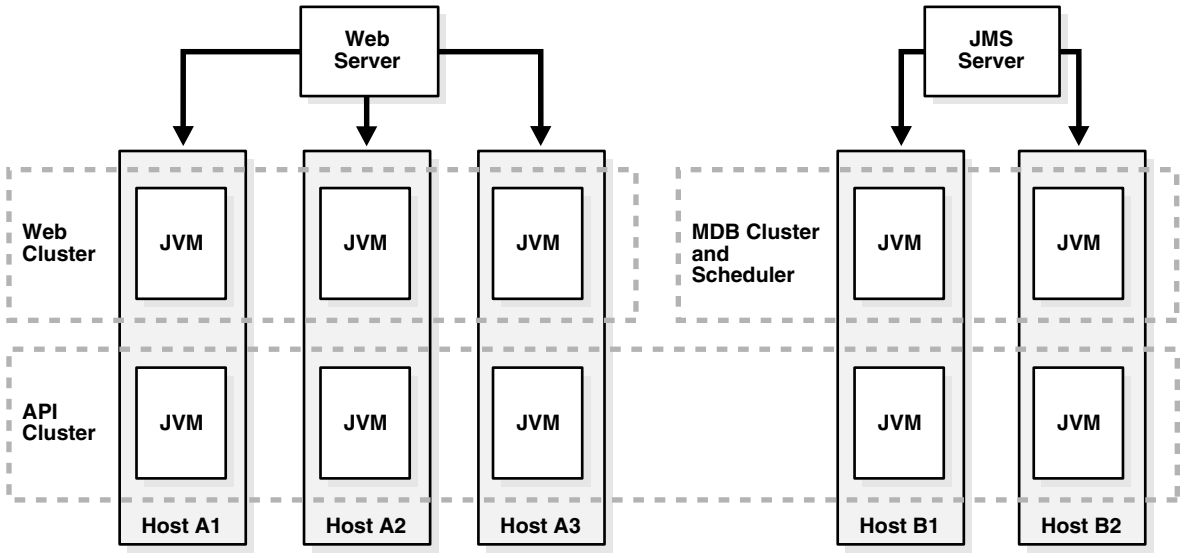
  It also restricts processing to the Front Office cluster. For example, off-lining task approvals occur in the Front Office cluster.

9.21 Multiple Clustered Installation

After installing Oracle Identity Manager in a multiple-clustered environment, in which clusters share the same Node Domain Manager (NDM), you can add more servers and create more clusters. You can also map modules to different clusters by using the WebSphere administrative console.

Figure 9–3 shows that the multiple-clustered environment is hosting different modules. If you want to configure a computer (host) for multiple functions, then you can map multiple modules to this host.

Figure 9–3 Multiple Oracle Identity Manager Cluster Environments Hosting Different Modules



Note: When creating the Oracle Identity Manager Cluster by using the WebSphere administrative console, ensure that you select the **Prefer Local** option so that the local EJBs are preferred over the remote EJBs.

9.21.1 Environment Advantages

The following are the advantages of the multiple-clustered environment:

- Multiple-clustered environment has the ability to load balance processing in which the Back Office cluster can take on the work, and vice versa.

  For example, there are times when the API cluster on the Front Office can process scheduled tasks.

- The Back Office cluster represents a true Back Office in which designated off-lined tasks are processed within the Back Office computers.
- The Design Console points to the same cluster for all operations.
- There is a central administration of the WebSphere cluster.

9.21.2 Environment Disadvantages

The following are the disadvantages of the multiple-clustered environment:

- Multiple JVMs run on all the computers within the cluster.

  The impact on performance is unknown.

- After applying patches, you must perform manual steps to map modules into the proper cluster because the current patch mechanism cannot accommodate the two separate deployments.

9.21.3 Installation Considerations

The following are the installation considerations in a multiple-clustered environment:

- Install WebSphere by following the clustered installation steps in this guide, but name the cluster XL_API_CLUSTER instead of XL_CLUSTER.
- Create additional clusters: XL_API_CLUSTER, WebCluster, and BackOfficeCluster.

  Add servers into the clusters by using the same model server for all of them.
- In the Web cluster, add servers into the nodes participating in the Front Office.

  Note: To indicate that the server is hosting Web components, append the word "Web" to the end of the server name. For example, Node1Server1Web.

  a. In the Back Office cluster, add servers into the nodes participating in the Back Office. Use the suffix, BackOffice or BO.

  b. Create servers in XL_API_CLUSTER and add the suffix API to the servers.
- Map modules into different clusters:

  a. Click **Enterprise Applications**, and then click **Oracle Identity Manager**.

  b. Click **Map modules to Application Servers**.

  c. Select **xlWebApp.war**, and then select the **WebCluster** from the list on the top.

  d. Click **Apply**. xlWebApp.war runs on Web Cluster.

  e. Select **xlBackOfficeBeans**, **xlScheduler.war**, and **SchedulerBean**, and then map them to the BackOffice cluster.

  f. Save the changes.
- Modify xlconfig.xml and change the Discovery section. Include the boot strap ports of the correct servers to find the various components.

  a. Edit the websphere.profile and ensure that the cluster name is XL_API_CLUSTER.

  b. Run websphereConfigUtility.cmd to get the list URL to be used for CoreServer component.

  c. Perform the same steps for BackOfficeCluster to get the JNDI URL to be used for BackOffice, Scheduler, and JMSServer components.
- Start all the clusters.
- Restart the application.

9.21.4 Scaling

Follow these guidelines when scaling up your environment:

- To add more computers to handle Front Office requests, add a new node, and then add servers in both the WebCluster and the API Cluster.
- To add more processing power in the Back Office cluster, add a new node, and then add servers to the API Cluster and the Back Office Cluster on that node.

9.21.5 Variation

It is possible to keep Web and API on the same cluster so that only one JVM is running on the Front Office computers. On the other hand, the generated plug-in configuration must be modified to remove the Back Office computers.

9.22 Setting Up Supported Integrations on a WebSphere Cluster

To deploy an Oracle Identity Manager-supported integration on the WebSphere clustered environment, you must ensure that the integration is accessible for all cluster members. See the Oracle Identity Manager Connectors documentation set located on Oracle Technology Network to learn about supported connectors for Oracle Identity Manager.

9.22.1 Shared Directory

During the Oracle Identity Manager installation, the Oracle Identity Manager folder, Oracle by default, is generated. This folder contains configuration information, for example, third-party libraries, keystores, scheduled tasks, and adapter classes. In a WebSphere clustered environment, ensure that this folder is installed as a shared folder and is centrally located so that all cluster members can access the latest configuration information referenced by the application server.

Note: Refer to the "Installing Oracle Identity Manager Cluster By Using a Shared Directory" section on page 9-31 for more information.

9.22.2 Using SSL

For any Oracle Identity Manager-supported integrations that are deployed by using a Secure Sockets Layer (SSL) connection between the target system, for example Active Directory, and the clustered WebSphere application server, you must import the target system SSL certificate file into the trusted store for each cluster member computer.

For a standard WebSphere deployment, the target system SSL certificate must be imported to *WEBSPHERE_HOME*`/etc/DummyServerTrustFile.jks`. The default password for this file is WebAS. In a customized WebSphere deployment in which a different trusted store is used, you must import the target system SSL certificate to that store.

9.22.3 Time Synchronization of Clustered Machines

Ensure that all cluster members have their system clocks synchronized. Oracle recommends that you do not run clustering on separate computers unless their system clocks are synchronized by using some form of time-sync service (daemon) that runs frequently. The clocks must be within a second of each other. Visit `http://www.boulder.nist.gov/timefreq/service/its.htm` for more information by using the time-sync service.

Caution: Never start a nonclustered instance against the same set of tables that another instance is running against. You will experience serious data corruption and erratic behavior.

9.23 Postinstallation Configuration for Clustered Installations

After completing the steps in this chapter, ensure that you perform the postinstallation configuration tasks for the clustered environment by referring to the "Postinstallation Configuration for Oracle Identity Manager and IBM WebSphere Application Server" section on page 7-1 to complete the cluster deployment.

10

Installing and Configuring the Oracle Identity Manager Design Console

This chapter explains how to install the Oracle Identity Manager Design Console Java client. You can install the Design Console on the same computer in which Oracle Identity Manager is installed or on a separate computer.

This chapter discusses the following topics:

10.1 Requirements for Installing the Design Console

Verify that your system environment meets the following requirements for Design Console installation:

- You must have a running installation of Oracle Identity Manager.
- If you are installing on a computer other than the host for the application server, then you must know the host name and port number of the computer hosting that application server.
- The Design Console host must be able to ping the application server host by using both IP and host name.
- For a clustered Oracle Identity Manager installation, you must know the host name and port number of the Web server.

> **Note:** If you cannot resolve the host name of the application server, then try adding the host name and IP address in the hosts file in the `C:\winnt\system32\drivers\etc\` directory.

- The Design Console must be installed on the same computer as the IBM WebSphere Client Application.

- Ensure that the WebSphere Application Client is configured with the appropriate server certificate.

  Refer to the "Setting Environment Variables" section on page 3-4 for more information.

- Ensure that the complete JRE is installed for WebSphere Application Client in the same way as it is for the Application Server JRE installation. A valid and complete WebSphere Application Client installation includes a java directory. If this java directory does not exist for the WebSphere Application Client installation, then create it by copying it from the WebSphere Application Server installation.

10.2 Installing the Design Console

This section describes how to install the Design Console.

> **Note:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Design Console on a computer that is hosting another Oracle Identity Manager component, such as Oracle Identity Manager or the Remote Manager, then you must specify a different installation directory for the Design Console.

To install the Design Console on a Microsoft Windows host:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Using Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the **setup_client.exe** file.
4. Choose a language from the list on the Installer page.

   The Welcome page is displayed.
5. In the Welcome page, click **Next**.
6. In the Target directory page, complete one of the following steps:
   - The default directory for the Design Console is `C:\oracle`. To install the Design Console into this directory, click **Next**.
   - To install the Design Console into another directory, enter the path in the Directory field, then click **Next**. Alternatively, you can click **Browse**, navigate to the desired location, and then click **Next**.

   > **Note:** If the directory path that you specified does not exist, then the Base Directory settings field is displayed. Click **OK**. The directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message, and then contact your system administrator to obtain the appropriate permissions.

7. In the Application Server page, select **WebSphere**, and then click **Next**.

8. In the IBM Websphere Directory page, enter the location of Websphere Application Client directory, and then click **Next**.
9. In the Application Server configuration page, enter the information appropriate for the application server hosting Oracle Identity Manager, as follows:
   a. In the first field, enter the host name or IP address in the upper field.
   b. In the second field, enter the bootstrap naming port for the application server on which Oracle Identity Manager is deployed.

   Note:

   - The host name is case-sensitive.
   - To find the bootstrap naming port, open `AboutThisProfile.txt` in *`WEBSPHERE_HOME`*`/profiles/`*`PROFILE_NAME`*`/logs`.

   c. Click **Next**.
10. In the Graphical Workflow Rendering Information page, enter the Application server configuration information:
    a. Enter the Oracle Identity Manager server (host) IP address. For a clustered environment, enter the IIS server IP address.
    b. Enter the port number. For a clustered environment, enter the IIS server port number.
    c. Select **Yes** or **No** to specify whether or not the Design Console must use Secure Sockets Layer (SSL).
    d. Click **Next**.
11. In the **Shortcut** page, select the shortcut options according to your preferences:
    a. Choose to create a shortcut to the Design Console on the Start menu.
    b. Choose to create a shortcut to the Design Console on the desktop.
    c. After completing the settings, click **Next**.
12. In the Summary page, click **Install** to start the Design Console installation.
13. The final installation page displays a reminder to copy certain application server-specific files to the Oracle Identity Manager installation.

    Follow these instructions and then click **OK**.
14. Click **Finish** to complete the installation.

10.3 Postinstallation Requirements for the Design Console

To run the Design Console, a JAR file must be copied from the WebSphere

Application Server installation to your Design Console installation. The jar file must be extracted from the Oracle Identity Manager EAR file. Perform the following steps:

1. Extract the xlDataObjectBeans.jar file from the Oracle Identity Manager EAR file.
2. Copy xlDataObjectBeans.jar into the following directory:

   `OIM_DC_HOME``\xlclient\lib`

Click **OK** to replace the old xlDataObjectBeans.jar file.

3. In the configuration XML file, change the multicast address to match that of Oracle Identity Manager:

   a. Open the following file:

      OIM_HOME\xellerate\config\xlconfig.xml

   b. Search for the <MultiCastAddress> element, and copy the value assigned to this element.

   c. Open the following file:

      OIM_DC_HOME\xlclient\Config\xlconfig.xml

   d. Search for the <Cache> element, and replace the value of the <MultiCastAddress> element inside this element with the value that you copy in Step b.

10.3.1 Extracting xlDataObjectBeans.jar

To obtain the EAR file, export it from the WebSphere server by using the WebSphere administrative console. You must also extract the xlDataObjectBeans.jar file from the EAR file so that you can copy the JAR file to the lib directory of the Oracle Identity Manager Design Console.

To extract the xlDataObjectBeans.jar file:

1. Using a Web browser, connect to the WebSphere administrative console by navigating to the following URL:

   http://*NDM_HOST*/*NDM_PORT*/admin

2. Log in by using Oracle Identity Manager Administrator name and password you specified during installation.
3. Click **Applications**, and then select **Enterprise Applications**.
4. Select **Xellerate application**.
5. Click **Export**.
6. Save the EAR file.
7. Extract the xlDataObjectBeans.jar file. Ensure that you extract xlDataObjectBeans.jar and not xlDataObjects.jar.

10.3.2 Configuring the WebSphere Application Client in a Nonclustered Environment

The certificate for the application server must be installed in the trusted store for the WebSphere AppClient. This required step establishes a trust relationship between the WebSphere server and client. Use the keytool included with WebSphere to perform this task.

Note: If you use the default WebSphere certificate, then this task is not necessary because the certificate is already present in the keystore of the client.

To enable trust between the server and client:

1. Move to the *WEBSPHERE_HOME*\etc directory by using the following command:

```
cd WEBSPHERE_HOME\etc
```

2. Export the server certificate by using the following commands:

```
WEBSPHERE_HOME\java\jre\bin\keytool.exe -export
-alias server -keystore DummyServerKeyFile.jks
-storepass WebAS -file servercert
```

3. Copy the exported server certificate to the *WEBSPHERE_CLIENT_HOME*/etc directory on the client host computer. *WEBSPHERE_CLIENT_HOME* is the home directory of the WebSphere client. Typically, the home directory is *WEBSPHERE_INSTALL_DIR*/AppClient.

4. Import the server certificate into the trusted store for the client by using the following commands, or similar commands appropriate for your system:

   a. Go to the *WEBSPHERE_CLIENT_HOME*/etc directory by using the following command:

```
cd WEBSPHERE_CLIENT_HOME/etc
```

   b. Import the server certificate by using the following command:

```
WEBSPHERE_CLIENT_HOME\java\jre\bin\keytool.exe -import -alias servertrust
-trustcacerts -keystore DummyClientTrustFile.jks -storepass WebAS -file
servercert
```

Note: If the *WEBSPHERE_CLIENT_HOME* directory does not contain the complete java directory when compared with the java directory inside the WebSphere Application Server installation directory, then copy the java directory from the WebSphere Application Server installation.

10.3.3 Configuring the Design Console in a WebSphere Cluster

If you are running Oracle Identity Manager in a WebSphere cluster, then you must configure the Design Console. During deployment, you update the JNDI references for each of the Nodes. You must also update the JNDI references for the Design Console.

To specify the JNDI URL for the Design Console:

1. On the computer that hosts the Design Console, open the *OIM_DC_HOME*/xlclient/Config/xlconfig.xml file.
2. In the <Discovery> section, locate the java.naming.provider.url property.
3. Set this property to the JNDI URL.

   Refer to the "Updating the JNDI References" section on page 9-26 for information about how to obtain this value. For example, you could set the property to the following:

```
<java.naming.provider.url>corbaloc:iiop:XL_NODE1_HOST:
9812,:XL_NODE2_HOST:9813</java.naming.provider.url>
```

4. Save the changes.
5. Start or restart the Design Console.

10.3.4 Configuring WebSphere Client Communication with the Node Manager in Clusters

The certificate of the Node Manager must be installed in the trusted store of the WebSphere Client. This step is necessary to establish a trust relationship between the Node Manager server and WebSphere Application Client. Use the keytool included with WebSphere to perform this task.

To enable trust relationship between the Node Manager and client:

1. Go to the Network Deployment Manager Host and change directory to *WEBSPHERE_SERVER_HOME*\profiles\XL_MANAGER_PROFILES\etc by using the following command:

   ```
   cd WEBSPHERE_SERVER_HOME\profiles\XL_MANAGER_PROFILES\etc
   ```

2. Export the server certificate by using the following commands:

   ```
   WEBSPHERE SERVER_HOME\java\jre\bin\keytool.exe -export
   -alias server -keystore DummyServerKeyFile.jks
   -storepass WebAS -file servercert
   ```

3. Copy the exported server certificate to the client host computer.

4. Import the Node Manager certificate into the client's trusted store by using the following commands. *WEBSPHERE_CLIENT_HOME* is the home directory for the WebSphere Client, which is usually \WebSphere\AppClient\.

   a. Go to the *WEBSPHERE_CLIENT_HOME*\etc directory by using the following command:

      ```
      cd WEBSPHERE_CLIENT_HOME\etc
      ```

   b. Import the Node Manager certificate into the client's trusted store by using the following command:

      ```
      WEBSPHERE_CLIENT_HOME\java\jre\bin\keytool.exe -import
      -alias servertrust -trustcacerts -keystore DummyClientTrustFile.jks
      -storepass WebAS -file
      servercert
      ```

10.4 Starting the Design Console

To start the Design Console, double-click *OIM_DC_HOME*\xlclient\wsxlclient.cmd or select Design Console from the Windows Start menu or desktop.

When the design console starts for the first time, it prompts whether to import certificates from the server. At the prompt, enter **y**.

Note: For non-English installations, irrespective of the prompt, only **y** works.

For example, in German language installations, you are prompted with the options j/n, but entering j will not work.

10.5 Setting the Compiler Path for Adapter Compilation

In the System Configuration form of the Design Console, you must set the XL.CompilerPath system property to include the path of the bin directory inside the

JDK directory (*JDK_HOME*\bin) that is used by the application server on which Oracle Identity Manager is deployed.

Then, restart Oracle Identity Manager.

> **See Also:** The "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference*

10.6 Configuring SSL Communication With the Design Console (Optional)

After installing the Oracle Identity Manager Design Console, you might want to configure it to communicate to Oracle Identity Manager over SSL. The following sections discuss how to configure the communication from the Design Console to Oracle Identity Manager over SSL:

- Configuring WebSphere
- Configuring the Design Console
- Configuring the Administrative and User Console (Optional)
- Configuring Non-Default Certificates

10.6.1 Configuring WebSphere

To configure WebSphere:

1. Start the WebSphere Administrative Console and log in.
2. Go to **Security**, **Secure administration, applications, and infrastructure**, **RMI-IIOP Security Under Authentication**, and then **CSIv2 Inbound Transport**.
3. For the Transport settings, select **SSL-Supported.**
4. Go to **Security**, **Authentication Protocol**, and then **CSIv2 Outbound Transpot**.
5. For the Transport settings, select **SSL-Supported.**
6. Save the configuration and then restart the application server.

10.6.2 Configuring the Design Console

To configure the Design Console:

1. Open the *OIM_DC_HOME*/xlclient/wsxlclient.cmd file.
2. To the existing properties, add the following or ensure that the following is already specified):

   ```
   CCDcom.ibm.CORBA.ConfigURL="file:%WS_HOME%/properties/sas.client.props"
   ```

3. Open the "%WS_HOME%"/properties/sas.client.properties file.
4. Make the following changes in the properties:

   ```
   com.ibm.CSI.performMessageIntegrityRequired=true

   com.ibm.CSI.performMessageIntegritySupported=true

   com.ibm.CSI.performTransportAssocSSLTLSSupported=true

   com.ibm.CSI.performTransportAssocSSLTLSRequired=true
   ```

5. Open the *OIM_DC_HOME*/xlclient/Config/xlconfig.xml file.

6. Modify the <ApplicationURL> value to use SSL as in the following example:

   Change:

   http://*WAS_HOST_NAME*:9080/xlWebApp/loginWorkflowRenderer.do

   To:

   https://*WAS_HOST_NAME*:9443/xlWebApp/loginWorkflowRenderer.do

---

Note: The modifications apply only to the protocol and the port number. The port number is modified assuming that the server is configured with default port numbers.

If you have changed the default port numbers, then use the same port number accordingly.

To find the SSL port for the server,

1. Log on to the WebSphere Administrative Console.
2. Navigate to **Servers**, **Application Servers**, ***server name***, **Communications**, and then **Ports**.

WC_defaulthost_secure is the SSL port, and WC_defaulthost is the non-SSL port for the application server.

Note: For clustered installations of WebSphere with a Web server, the Web server certificate must be trusted with the Design Console trust store for enabling SSL communication. After this is done, you can select one of the servers in the cluster for HTTPS connections as follows:

https://*WEBSERVER_HOST_NAME*:*SSL_PORT*/xlWebApp/loginWorkflowRenderer.do

Alternatively, you can also select one of the servers in the cluster for HTTPS connections, as follows:

https://*APPSERVER1_HOST_NAME*:*SSL_PORT*/xlWebApp/loginWorkflowRenderer.do

---

10.6.3 Configuring the Administrative and User Console (Optional)

After configuring WebSphere and the Design Console, you can access the application by using SSL and non-SSL ports.

To access the application securely by using SSL, you must use port number 9443 or WC_defaulthost_secure .

Example: https://localhost:9443/xlWebApp

To access the application in a non-secure mode, use port number 9080 or WC_defaulthost.

Example: http://localhost:9080/xlWebApp

10.6.4 Configuring Non-Default Certificates

The "Configuring WebSphere", "Configuring the Design Console" section and the "Configuring the Administrative and User Console (Optional)" section describe how to configure SSL by using the default certificates provided by WebSphere.

For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords.

If you create a new keystore or truststore with different passwords, then you must modify the encrypted old password in `sas.client.properties` with the new clear-text password.

To encrypt the clear-text password, use the utility `PropFilePasswordEncoder.bat` available at the following location:

`WebSphere_Home/bin.`

Ensure that you use the SAS option.

> **Note:** Refer to the WebSphere documentation for more information about creating certificates and configuring trust and keystores. Otherwise, contact IBM support.

10.7 Removing the Design Console Installation

To remove the Design Console installation:

1. Stop Oracle Identity Manager and the Design Console if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the *`OIM_DC_HOME`* directory in which you installed the Design Console.

11

Installing and Configuring the Oracle Identity Manager Remote Manager

This chapter explains how to install Oracle Identity Manager Remote Manager. It discusses the following sections:

11.1 Installing the Remote Manager for Microsoft Windows

To install the Remote Manager on a Microsoft Windows host:

> **Note:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a computer that is hosting another Oracle Identity Manager component, such as the server or the Design Console, then specify an installation directory that has not been used.

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Using Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the **setup_rm.exe** file.
4. Choose a language from the list on the Installer page. The Welcome page is displayed.
5. In the Welcome page, click **Next**.
6. In the Target directory page, complete one of the following steps:
   - The default directory for Oracle Identity Manager products is `C:\oracle`. To install the Remote Manager into this directory, click **Next**.
   - To install Remote Manager in a different directory, specify the path of the directory in the **Directory name** field, and then click **Next**.

Note: If the directory path that you specified does not exist, then the Base Directory settings field is displayed. Click **OK**. The directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message, and then contact your system administrator to obtain the appropriate permissions.

7. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Click **Next**. The Remote Manager Configuration page is displayed.
8. In the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Enter the service name. The default value is RManager.
   b. Enter the Remote Manager binding port. The default value is 12346.
   c. Enter the Remote Manager Secure Sockets Layer (SSL) port. The default value is 12345.
   d. Click **Next**.
9. In the **Shortcut** page, select the check boxes for the shortcut options according to your preferences:
   a. Choose to create a shortcut for the Remote Manager on the desktop.
   b. Choose to create a shortcut for the Remote Manager on the Start Menu.
   c. Click **Next** after completing the check box settings.
10. In the Summary page, review the configuration details, and then click **Install** to start the installation.
11. Click **Finish** to complete the installation.

Note: You must configure the Remote Manager before you can start it. Refer to the "Configuring the Remote Manager" section on page 11-4 for more information about configuring the Remote Manager.

11.2 Installing the Remote Manager for UNIX or Linux

To install the Remote Manager on UNIX or Linux:

1. Before installing the Remote Manager, you must set the JAVA_Home variable to the appropriate JDK.

   On Solaris or Linux, set JAVA_HOME to the Sun JDK. On AIX, set JAVA_HOME to the WebSphere JDK. For example, use the following commands on AIX:

   - `export JAVA_HOME=$WEBSPHERE_HOME/java`
   - Add `$JAVA_HOME/bin to the $PATH` environment variable by using the following command:

     ```
     export PATH=$JAVA_HOME/bin:$PATH
     ```

See Also: *Oracle Identity Manager Readme* for information about the certified JDK versions

2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

   Note: If the autostart routine is enabled for your computer, proceed to Step 5.

3. From the File Manager, access the root CD directory or the installServer directory, if you are installing from a tar file.
4. Run the install_rm.sh file.

   The command-line installer starts.
5. Choose a language from the list by entering a number and then by entering **0** to apply the language.

   The Welcome panel is displayed.
6. In the Welcome panel, enter **1** to move to the next panel.

   The Target directory panel is displayed
7. In the Target directory panel, enter the path to the directory in which you want to install the Remote Manager. The default directory is `/opt/oracle`.
   - Enter **1** to move to the next panel.
   - If the directory does not exist, then you are asked to create it. Enter **y** for yes.

   Note: All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a computer that is hosting Oracle Identity Manager, then you must specify a unique installation directory.

8. Specify the JRE to use with the Remote Manager, and then:
   - Enter **1** to install the JRE included with Oracle Identity Manager.
   - Enter **2** to use an existing JRE at a specified location.

   After specifying the JRE, enter **0** to accept your selection and then enter **1** to move to the next panel.
9. In the Remote Manager Configuration panel, enter the Remote Manager configuration information as follows:
   a. Enter the Service Name, or press the **Enter** key to accept the default.
   b. Enter the Remote Manager binding port, or press the **Enter** key to accept the default.
   c. Enter the Remote Manager SSL port, or press the **Enter** key to accept the default.
   d. Enter **1** to move to the next panel.

   The Remote Manager installation summary panel is displayed.
10. Check the information, and then:

- Enter **2** to go back and make changes.
- Enter **1** to start the installation.

Oracle Identity Manager installs and the Post Install Summary panel is displayed.

11. Enter **3** to finish the Remote Manager installation.

Note: You must configure the Remote Manager before you can start it. Refer to the "Configuring the Remote Manager" section on page 11-4 for more information.

11.3 Configuring the Remote Manager

The Remote Manager and Oracle Identity Manager communicate by using SSL. If you are using the Remote Manager, then you must enable a trust relationship between Oracle Identity Manager and the Remote Manager. The server must trust the Remote Manager certificate.

Optionally, you can enable client-side authentication in which the Remote Manager checks the server certificate. Import the Remote Manager certificate into the Oracle Identity Manager keystore and make it trusted. For client-side authentication, import the certificate for Oracle Identity Manager into the keystore for the Remote Manager, and then make that certificate trusted. You must also manually edit the configuration file associated with the server, and depending on the options you selected during Remote Manager installation, edit the Remote Manager configuration file as well.

11.3.1 Changing the Remote Manager Keystore Passwords

During installation, the password for the Remote Manager keystore is set to `xellerate`. Oracle recommends that changing the keystore passwords for all production installations.

To change the keystore passwords, you must change the storepass of .xlkeystore and the keypass of the xell entry in .xlkeystore, and these two values must be identical. Use the keytool and perform the following steps to change the keystore passwords:

1. Open a command prompt on the Oracle Identity Manager host computer.
2. Navigate to the *OIM_RM_HOME*`\xellerate\config` directory.
3. Run the keytool with the following options to change the storepass:

   ```
   JAVA_HOME\jre\bin\keytool -storepasswd -new new_password -storepass xellerate
   -keystore .xlkeystore -storetype JKS
   ```

4. Run the keytool with the following options to change the keypass of the xell entry in .xlkeystore:

   ```
   JAVA_HOME\jre\bin\keytool -keypasswd -alias xell -keypass xellerate
   -new new_password -keystore .xlkeystore -storepass xellerate
   ```

   JAVA_HOME represents the location of the Java installation associated with the Remote Manager installation.

5. In a text editor, open the *OIM_RM_HOME*`\xlremote\config\xlconfig.xml` file.
6. Edit the `<RMSecurity>.<KeyStore>` section to specify the keystore password as follows:

- Change the password tag to `encrypted=false`.
- Enter the password, for example:

```
<RMSecurity>
<KeyStore>
<Location>.xlkeystore</Location>
<Password encrypted="false">new_password</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

Note: If you are using client-side authentication for the Remote Manager, then enter the Oracle Identity Manager keystore password in the `<RMSecurity>.<TrustStore>` section of *OIM_RM_HOME*`\xlremote\config\xlconfig.xml` as follows:

```
<TrustStore>
<Location>.xlkeystore</Location>
<Password encrypted="false">OIM_Server_keystore_password</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</TrustStore>
```

---

7. Save and close the xlconfig.xml file.
8. Restart the Remote Manager.
9. In a text editor, open the *OIM_HOME*`\xellerate\config\xlconfig.xml` file.
10. Edit the `<RMSecurity>.<TrustStore>` section to specify the new Remote Manager keystore password as follows:
    - Change the password tag to `encrypted=false`.
    - Enter the password, for example:

```
<TrustStore>
<Location>.xlkeystore</Location>
<Password encrypted="false">new_password</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</TrustStore>
```

11. Save and close the xlconfig.xml file, then restart Oracle Identity Manager.

11.3.2 Trusting the Remote Manager Certificate

To establish a trust relationship between Oracle Identity Manager and the Remote Manager:

1. Copy the Remote Manager certificate to the server computer.

   On the Remote Manager computer, locate the *OIM_RM_HOME*`\xlremote\config\xlserver.cert` file and copy it to the server computer.

Note: The server certificate located in *OIM_HOME*\config is also named xlserver.cert. Ensure that you do not overwrite that certificate.

2. Open a command prompt on the server computer.
3. To import the certificate by using the keytool utility, use the following command:

```
JAVA_HOME\jre\bin\keytool -import -alias
rm_trusted_cert -file RM_cert_location\xlserver.cert
-trustcacerts -keystore
OIM_HOME\xellerate\config\.xlkeystore -storepass
xellerate
```

JAVA_HOME is the location of the Java directory for the application server, the value of alias is an arbitrary name for the certificate in the store, and *RM_cert_location* is the location in which you copied the certificate.

Note: If you changed the keystore password, then substitute that value instead of xellerate for the value of the storepass variable.

4. Enter **Y** at the prompt to trust the certificate.
5. In a text editor, open the *OIM_HOME*\xellerate\config\xlconfig.xml file.
6. Locate the property <RMIOverSSL> and set it to true.

   For example:

```
<RMIOverSSL>true</RMIOverSSL>
```

7. Locate the <KeyManagerFactory> property.

   If you are using the IBM JRE, then set the value to IBMX509. For all other JREs, set the value to SUNX509. For example:

```
<KeyManagerFactory>IBMX509</KeyManagerFactory>
```

   Or:

```
<KeyManagerFactory>SUNX509</KeyManagerFactory>
```

8. Save the file.
9. Restart Oracle Identity Manager.

11.3.2.1 Using Your Own Certificate

To configure the Remote Manager by using your own certificate on the Remote Manager system:

1. Import your custom key in a new keystore (new_keystore_name) other than .xlkeystore. Remember the password (new_keystore_pwd) that you use for the new keystore.
2. Copy this new keystore to the *OIM_RM_HOME*\xlremote\config\ directory.
3. In a text editor, open the *OIM_RM_HOME*\xlremote\config\xlconfig.xml file.

4. Locate the <RMSecurity> tag and change the value in the <Location> and <Password> tags as follows:

   - If you are using the IBM JRE, then change the values to:

```
<KeyStore>
     <Location>new_keystore_name</Location>
     <Password encrypted="false">new_keystore_pwd</Password>
     <Type>JKS</Type>
     <Provider>com.ibm.crypto.provider.IBMJCE</Provider>
</KeyStore>
```

   - For all other JREs, change the values to:

```
<KeyStore>
     <Location>new_keystore_name</Location>
     <Password encrypted="false">new_keystore_pwd</Password>
     <Type>JKS</Type>
     <Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

5. Restart the Remote Manager server, and open the xlconfig.xml file to ensure that the password for the new keystore was encrypted.

To configure the Remote Manager by using your own certificate on the Oracle Identity Manager server:

1. Import the same certificate key used in the Remote Manager system to a new keystore (new_svrkeystore_name) other than .xlkeystore. Remember the password (new_svrkeystor_pwd) that you use for the new keystore.
2. Copy this new keystore to the *OIM_HOME*\xellerate\config directory.
3. In a text editor, open the *OIM_HOME*\xellerate\config\xlconfig.xml file.
4. Locate the <RMSecurity> tag and change the value in the <Location> and <Password> tags as follows:

   - If you are using the IBM JRE, then change the values to:

```
<KeyStore>
     <Location>new_keystore_name</Location>
     <Password encrypted="false">new_keystore_pwd</Password>
     <Type>JKS</Type>
     <Provider>com.ibm.crypto.provider.IBMJCE</Provider>
</KeyStore>
```

   - For all other JREs, change the values to:

```
<KeyStore>
     <Location>new_keystore_name</Location>
     <Password encrypted="false">new_keystore_pwd</Password>
     <Type>JKS</Type>
     <Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

5. Restart Oracle Identity Manager and open the xlconfig.xml file to ensure that the password for the new keystore is encrypted.

11.3.3 Enabling Client-Side Authentication for Remote Manager

To enable client-side authentication:

1. On the computer hosting the Remote Manager, in a text editor, open the *OIM_RM_HOME*\xlremote\config\xlconfig.xml file.
2. Locate the <ClientAuth> property and set it to true, for example:

   ```
   <ClientAuth>true</ClientAuth>
   ```

3. Locate the <RMIOverSSL> property and verify it is set to true, for example:

   ```
   <RMIOverSSL>true</RMIOverSSL>
   ```

4. Locate the <KeyManagerFactory> property.

   If you are using the IBM JRE, then set the value to IBMX509. For all other JREs, set the value to SUNX509. For example:

   ```
   <KeyManagerFactory>IBMX509</KeyManagerFactory>
   ```

   Or:

   ```
   <KeyManagerFactory>SUNX509</KeyManagerFactory>
   ```

5. Save the *OIM_RM_HOME*\xlremote\config\xlconfig.xml file.
6. Copy the server certificate to the Remote Manager computer.

   On the server computer, locate the *OIM_HOME*\xellerate\config\xlserver.cert file and copy it to the Remote Manager computer.

   Note: The Remote Manager certificate is also named xlserver.cert. Ensure that you do not overwrite that certificate.

7. Open a command prompt on the Remote Manager computer.
8. Import the certificate by using the following keytool command:

   ```
   JAVA_HOME\jre\bin\keytool -import -alias
   trusted_server_cert -file
   server_cert_location\xlserver.cert -trustcacerts
   -keystore OIM_RM_HOME\xlremote\config\.xlkeystore
   -storepass xellerate
   ```

   JAVA_HOME is the location of the Java directory for the Remote Manager, the value of alias is an arbitrary name for the certificate in the store, *OIM_RM_HOME* is the home directory for the Remote Manager, and *server_cert_location* is the location in which you copied the server certificate.

   Note: If you changed the keystore password, then substitute that value for xellerate, which is the default value of the storepass variable.

9. Enter **Y** at the prompt to trust the certificate.
10. Restart the Remote Manager.

11.4 Starting the Remote Manager

Use the following script to start the Remote Manager:

- On Microsoft Windows:

OIM_RM_HOME\xlremote\remotemanager.bat

- On UNIX:

  OIM_RM_HOME/xlremote/remotemanager.sh

11.5 Removing the Remote Manager Installation

To remove the Remote Manager installation:

1. Stop Oracle Identity Manager and the Remote Manager if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the *OIM_RM_HOME* directory in which you installed the Remote Manager.

12

Troubleshooting the Oracle Identity Manager Installation

This section describes the following problems that can occur during the Oracle Identity Manager installation:

- Task Scheduler fails in a Clustered Installation
- Default Login Does Not Work

> **Note:** You can use the Diagnostic Dashboard tool for assistance when you troubleshoot the Oracle Identity Manager Installation. See *Oracle Identity Manager Administrative and User Console Guide* for detailed information.

12.1 Task Scheduler fails in a Clustered Installation

The Task Scheduler fails to work properly when the cluster members, which are computers that are part of the cluster, have different settings on their system clocks. Oracle recommends that the system clocks for all cluster members be synchronized within a second of each other.

12.2 Default Login Does Not Work

If the default login does not work for the Design Console or Administrative and User Console and you are using Microsoft SQL Server, then:

- Ensure that the Distributed Transaction Coordinator is running.
- For WebSphere clustered and nonclustered installations, ensure that the application server's bootstrap port reflects correctly in `xlconfig.xml`. By default, both cluster and nonclustered installations of Oracle Identity Manager points to bootstrap port `2809` in `xlconfig.xml`. Edit this number and restart the WebSphere application servers.

> **Note:** This applies only if you have more than one WebSphere profile on a computer.

A

Java 2 Security Permissions for IBM WebSphere

This appendix describes the following:

- Java 2 Security Permissions for WebSphere Noncluster
- Java 2 Security Permissions for WebSphere Cluster

Note: The application might fail to start because of syntax errors in the policy files.

Be careful when you edit the policy files. Oracle recommends that you use the policy tool provided by the JDK for editing the policy files. The tool is available in the following directory:

WAS_HOME/jre/bin/policytool

A.1 Java 2 Security Permissions for WebSphere Noncluster

To enable Java 2 Security for Oracle Identity Manager running on IBM WebSphere Application Server:

1. Log in to the WebSphere Administrative Console.
2. Expand the Security tab in the left navigation pane and then click **Secure administration**, **applications**, and **infrastructure**.
3. Click the **Security Configuration Wizard** button. The Security Configuration Wizard is displayed.
4. In the Specify Extent of Protection page of the Wizard, select the **Use Java 2 security to restrict application access to local resources** option and then click **Next**.
5. In the Select User Repository page of Wizard, click **Next**.
6. In the Configure User Repository page of the Wizard, enter **XELSYSADM** in the Primary administrative user name field. Click **Next**.
7. In the Summary page, click **Finish**.
8. To store the setting as Master Settings, click the **Save** link in the message.
9. Save this configuration and click **Apply**.
10. Check if the *WAS_HOME*/profiles/AppSrv01/properties/server.policy exists. If the file exists, edit it and add the Java 2 Security permissions provided in the "Policy File" section on page A-2. If it does not exist, then create it.

Policy File

The `server.policy` file consists of the following code:

> **Note:**
>
> - The instructions to change the code in the policy file are given in comments, which are in bold font.
>
> - Ensure that you change the cell name in the code example to reflect the cell name on which you install Oracle Identity Manager. This example uses `STDLPC28Node02Cell` as the cell name.
>
> - This `server.policy` example is for UNIX installation. For Windows, ensure that you change `/` between the directories name to `\\` in every `permission java.io.FilePermission` property.
>
> - Ensure that you change the multicast IP `231.167.157.106` in this example to reflect the multicast IP address of the Oracle Identity Manager installation. You can find the Oracle Identity Manager multicast IP address in `xlconfig.xml`.

```
// ****************************************
//  WebSphere Server Security Policy
// ****************************************
//
// Application client permissions are specified in client.policy
// Warning: Deviating from this policy might result in unexpected
// AccessControlExceptions if a more "fine grain" policy is
// specified.
// The application policy is specified in app.policy (per node) and was.policy
// (per enterprise application).
//
// Allow to use sun tools
grant codeBase "file:${java.home}/../lib/tools.jar" {
  permission java.security.AllPermission;
};

// WebSphere system classes
grant codeBase "file:${was.install.root}/plugins/-" {
  permission java.security.AllPermission;
};

grant codeBase "file:${was.install.root}/lib/-" {
  permission java.security.AllPermission;
};

grant codeBase "file:${was.install.root}/classes/-" {
  permission java.security.AllPermission;
};

// Allow the WebSphere deploy tool all permissions
grant codeBase "file:${was.install.root}/deploytool/-" {
  permission java.security.AllPermission;
};

// Allow Channel Framework classes all permissions
grant codeBase "file:${was.install.root}/installedChannels/-" {
  permission java.security.AllPermission;
```

```
    };

    // WebSphere optional runtime classes
    grant codeBase "file:${was.install.root}/optionalLibraries/-" {
      permission java.security.AllPermission;
    };


    //
    // ****************************************
    // From here, the Oracle Identity Manager application permissions start
    // ****************************************

    // OIM codebase permissions
    // Change Cell "STDLPC28Node02Cell" Value in given code
    grant codeBase
"file:${user.install.root}/installedApps/STDLPC28Node02Cell/Xellerate.ear/-" {
      permission java.security.AllPermission;
    };

    // Change Cell "STDLPC28Node02Cell" Value in given code
          permission java.io.FilePermission
            "${user.install.root}/temp/STDLPC28Node02Cell/server1/-",
"read,write,delete";

    // Need read, write, and delete permissions on $OIM_HOME/config folder
    // to read various config files, write the
    // xlconfig.xml.{0,1,2..} files upon re-encryption and delete
    // the last xlconfig.xml if the numbers go above 9.

          permission java.io.FilePermission "${XL.HomeDir}/config/-",
            "read, write, delete";
          permission java.io.FilePermission "${XL.HomeDir}/-", "read";

    // Need read,write,delete permissions to generate adapter java
    // code, delete the .class file when the adapter is loaded into
    // the database
          permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
            "read,write,delete";

    // This is required by the connectors and connector installer
          permission java.io.FilePermission
            "${XL.HomeDir}/ConnectorDefaultDirectory/-", "read,write,delete";
          permission java.io.FilePermission
            "${XL.HomeDir}/connectorResources/-", "read,write,delete";

    // Must read Globalization resource bundle files for various
    // locales
          permission java.io.FilePermission
            "${XL.HomeDir}/customResources/-", "read";

    // Must read code from "JavaTasks", "ScheduleTask",
    // "ThirdParty", "EventHandlers" folder
          permission java.io.FilePermission
            "${XL.HomeDir}/EventHandlers/-", "read";
          permission java.io.FilePermission
            "${XL.HomeDir}/JavaTasks/-", "read";
          permission java.io.FilePermission
            "${XL.HomeDir}/ScheduleTask/-", "read";
          permission java.io.FilePermission
```

```
        "${XL.HomeDir}/ThirdParty/-", "read";

// Required by the Generic Technology connector
      permission java.io.FilePermission  "${XL.HomeDir}/GTC/-", "read";
      permission java.io.FilePermission "${java.home}/lib/-", "read";
      permission java.lang.RuntimePermission
        "accessClassInPackage.sun.security.action";


      // OIM server invokes the java compiler. You need "execute"
      // permissions on all files.
      permission java.io.FilePermission "<<ALL FILES>>", "execute";

      // Socket permissions
      // Allow all permissions on non-privileged sockets
      // The multicast address should be the same as the one in
      // xlconfig.xml for javagroups communication
      permission java.net.SocketPermission "*:1024-",
        "connect,listen,resolve,accept";

      // This IP address is a multicast address of the computer. Ensure
      // it is the same as that defined in xlConfig.xml.
      permission java.net.SocketPermission "231.167.157.106",
        "connect,accept,resolve";

      // Property permissions
      // Read and write Oracle Identity Manager properties
      // Read XL.*, java.* and log4j.* properties
      permission java.util.PropertyPermission "XL.HomeDir", "read";
      permission java.util.PropertyPermission "XL.*", "read";
      permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
      permission java.util.PropertyPermission "log4j.*", "read";
      permission java.util.PropertyPermission "user.dir", "read";
      permission java.util.PropertyPermission "file.encoding", "read";
      permission java.util.PropertyPermission "java.class.path", "read";
      permission java.util.PropertyPermission "java.ext.dirs", "read";
      permission java.util.PropertyPermission "java.library.path", "read";

      // Runtime permissions
      // The Oracle Identity Mamager server needs permissions
      // to create its own class loader, get the class loader,
      // modify threads and register shutdown hooks
      permission java.lang.RuntimePermission "createClassLoader";
      permission java.lang.RuntimePermission "getClassLoader";
      permission java.lang.RuntimePermission "setContextClassLoader";
      permission java.lang.RuntimePermission  "setFactory";
      permission java.lang.RuntimePermission "modifyThread";
      permission java.lang.RuntimePermission "modifyThreadGroup";
      permission java.lang.RuntimePermission "shutdownHooks";

      // The Oracle Identity Manager server needs runtime
      // permissions to generate and load classes in the
      // following packages. Also access the
      // declared members of a class.
      permission java.lang.RuntimePermission
        "defineClassInPackage.com.thortech.xl.adapterGlue.ScheduleItemEvents";
      permission java.lang.RuntimePermission
        "defineClassInPackage.com.thortech.xl.dataobj.rulegenerators";
      permission java.lang.RuntimePermission
        "defineClassInPackage.com.thortech.xl.adapterGlue";
```

```
        permission java.lang.RuntimePermission "accessDeclaredMembers";

        // Reflection permissions
        // Give permissions to access and invoke fields/methods from
        // reflected classes.
        permission java.lang.reflect.ReflectPermission "suppressAccessChecks";

        // Security permissions for Oracle Identity Manager server
        permission java.security.SecurityPermission "*";
        permission java.security.SecurityPermission "insertProvider.IBMJCE";
        permission javax.security.auth.AuthPermission "doAs";
        permission javax.security.auth.AuthPermission "doPrivileged";
        permission javax.security.auth.AuthPermission "getSubject";
        permission javax.security.auth.AuthPermission "modifyPrincipals";
        permission javax.security.auth.AuthPermission "createLoginContext";
        permission javax.security.auth.AuthPermission "getLoginConfiguration";
        permission javax.security.auth.AuthPermission "setLoginConfiguration";
        permission java.security.SecurityPermission
          "getProperty.policy.allowSystemProperty";
        permission java.security.SecurityPermission
          "getProperty.login.config.url.1";
        permission javax.security.auth.AuthPermission
          "refreshLoginConfiguration";

        // SSL permission (for remote manager)
        permission javax.net.ssl.SSLPermission  "getSSLSessionContext";

        // Serializable permissions
        permission java.io.SerializablePermission "enableSubstitution";
    };


    // Grant AllPermission to nexaweb-common.jar
    grant codeBase "file:${was.install.root}/lib/nexaweb-common.jar" {
        permission java.security.AllPermission;
    };

    // Grant AllPermission to wssec.jar
    grant codeBase "file:${was.install.root}/lib/wssec.jar" {
        permission java.security.AllPermission;
    };

    // Nexaweb server codebase permissions
    // Change Cell "STDLPC28Node02Cell" Value in given code
    grant codeBase
"file:${user.install.root}/installedApps/STDLPC28Node02Cell/Nexaweb.ear/-" {

    // File permissions
        permission java.io.FilePermission
"${user.install.root}/temp/STDLPC28Node02Cell/server1/-","read,write,delete";
        permission java.io.FilePermission
"${user.install.root}/installedApps/STDLPC28Node02Cell/Xellerate.ear/-", "read";
        permission java.io.FilePermission "${user.home}", "read, write";
        permission java.io.FilePermission
"${user.install.root}/installedApps/STDLPC28Node02Cell/Nexaweb.ear/-", "read";
        permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
          "read,write,delete";
        permission java.io.FilePermission "<<ALL FILES>>", "execute";

    // Property permissions
```

```
      permission java.util.PropertyPermission "user.dir", "read";
      permission java.util.PropertyPermission "*", "read,write";

// Runtime permissions
// Nexaweb server needs permissions to create its own class loader,
// get the class loader etc.
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "getClassLoader";
permission java.lang.RuntimePermission "setContextClassLoader";
permission java.lang.RuntimePermission "setFactory";
permission java.lang.RuntimePermission "shutdownHooks";

// Nexaweb server security permissions to load the Cryptix
// extension
permission java.security.SecurityPermission "insertProvider.Cryptix";

// Socket permissions
// Permissions on all non-privileged ports.
permission java.net.SocketPermission "*:1024-",
        "listen, connect, resolve";

// Security permissions
permission javax.security.auth.AuthPermission "doAs";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext";
permission java.lang.RuntimePermission "modifyThread";
permission java.lang.RuntimePermission
       "accessClassInPackage.sun.security.action";

};

// The following are permissions given to codebase in the
// Oracle Identity Manager server directory
grant codeBase "file:${XL.HomeDir}/-" {
      // File permissions
      permission java.io.FilePermission "${XL.HomeDir}/config/-", "read";
      permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-", "read";
      permission java.io.FilePermission "${XL.HomeDir}/ScheduleTasks/-",
        "read";
      permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-",
        "read";
      permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
        "read,write,delete";

      // Socket permissions
      permission java.net.SocketPermission "*:1024-",
        "connect,listen,resolve,accept";

      // Property permissions
      permission java.util.PropertyPermission "XL.HomeDir", "read";
      permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
      permission java.util.PropertyPermission "XL.*", "read";
      permission java.util.PropertyPermission "log4j.*", "read";
      permission java.util.PropertyPermission "user.dir", "read";

      // Security permissions
      permission javax.security.auth.AuthPermission "doAs";
      permission javax.security.auth.AuthPermission "modifyPrincipals";
      permission javax.security.auth.AuthPermission "createLoginContext";
      permission java.lang.RuntimePermission "modifyThread";
```

```
        permission java.lang.RuntimePermission
          "accessClassInPackage.sun.security.action";
    };

    // Default permissions granted to all domains
    grant {
    // "standard" properties that can be read by anyone

    permission java.util.PropertyPermission "java.version", "read";
    permission java.util.PropertyPermission "java.vendor", "read";
    permission java.util.PropertyPermission "java.vendor.url", "read";
    permission java.util.PropertyPermission "java.class.version", "read";
    permission java.util.PropertyPermission "os.name", "read";
    permission java.util.PropertyPermission "os.version", "read";
    permission java.util.PropertyPermission "os.arch", "read";
    permission java.util.PropertyPermission "file.separator", "read";
    permission java.util.PropertyPermission "path.separator", "read";
    permission java.util.PropertyPermission "line.separator", "read";

    permission java.util.PropertyPermission "java.specification.version",
            "read";
    permission java.util.PropertyPermission "java.specification.vendor",
            "read";
    permission java.util.PropertyPermission "java.specification.name",
            "read";

    permission java.util.PropertyPermission
            "java.vm.specification.version", "read";
    permission java.util.PropertyPermission
            "java.vm.specification.vendor", "read";
    permission java.util.PropertyPermission "java.vm.specification.name",
            "read";
    permission java.util.PropertyPermission "java.vm.version", "read";
    permission java.util.PropertyPermission "java.vm.vendor", "read";
    permission java.util.PropertyPermission "java.vm.name", "read";

    permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
    permission java.lang.RuntimePermission "accessDeclaredMembers";
    permission java.util.PropertyPermission "XL.*", "read";
    permission java.util.PropertyPermission "user.dir", "read";
    permission java.util.PropertyPermission "*", "read,write";

    permission java.lang.RuntimePermission "getClassLoader";
    permission java.lang.RuntimePermission "createClassLoader";
    permission java.lang.RuntimePermission "setContextClassLoader";
    permission java.util.PropertyPermission "nexaweb.logs", "read,write";

    permission java.lang.RuntimePermission "loadLibrary.*";
    permission java.lang.RuntimePermission "queuePrintJob";
    permission java.net.SocketPermission    "*", "connect";
    permission java.io.FilePermission     "<<ALL FILES>>", "read,write";
    permission java.lang.RuntimePermission   "modifyThreadGroup";
    permission javax.security.auth.AuthPermission "doAs";
    permission java.lang.RuntimePermission "modifyThread";
};
```

A.2 Java 2 Security Permissions for WebSphere Cluster

Note: The application might fail to start because of syntax errors in the policy files.

Be careful when editing the policy files. Oracle recommends that you use the policy tool provided by the JDK for editing the policy files. The tool is available in the following directory:

WAS_HOME/jre/bin/policytool

This section describes the Java 2 Security permissions for WebSphere in a clustered environment. To enable Java 2 Security for Oracle Identity Manager running on a WebSphere cluster:

1. Log in to the WebSphere Administrative Console.
2. Expand the Security tab in the left navigation pane and then click **Secure administration**, **applications**, and then **infrastructure**.
3. Click the **Security Configuration Wizard** button. The Security Configuration Wizard is displayed.
4. In the Specify Extent of Protection page of the Wizard, select the **Use Java 2 security to restrict application access to local resources** option.
5. In the Select User Repository page of Wizard, click **Next**.
6. In the Configure User Repository page of the Wizard, enter **XELSYSADM** in the Primary administrative user name field. Click **Next**.
7. In the Summary page, click **Finish**.
8. To store the setting as Master Settings, click **Save Link** in the message and click **Apply**.
9. Check if the *WAS_HOME*/profiles/<PROFILE_NAME>/properties/server.policy file exists. If the file exists, edit it and add the Java 2 Security permissions provided in the "Policy File" section on page A-8. If it does not exist, then create it. You must do this in every node in which Oracle Identity Manager is deployed.

Policy File

The server.policy file consists of the following code:

Note:

- The instructions to change the code in the policy file are given in comments, which are in bold font.

- Ensure that you change the cell name in the code example to reflect the cell name on which you install Oracle Identity Manager. This example uses `XL_CELL` as the cell name, `XL_NODE1` as the node name, and `XL_SERVER_ON_NODE_1` as the server name.

- This `server.policy` example is for UNIX installation. For Windows, ensure that you change `/` between the directories name to `\\` in every `permission java.io.FilePermission` property.

- Ensure that you change the multicast IP `231.145.165.117` in this example to reflect the multicast IP address of the Oracle Identity Manager installation. You can find the Oracle Identity Manager multicast IP address in `xlconfig.xml`.

```
    //  WebSphere Server Security Policy
    //
    // Application client permissions are specified in client.policy
    // Warning: Deviating from this policy might result in unexpected
    // AccessControlExceptions if a more "fine grain" policy is
    // specified.
    // The application policy is specified in app.policy (per node) and was.policy
    // (per enterprise application).
    //
    // Allow to use sun tools
grant codeBase "file:${java.home}/../lib/tools.jar" {
  permission java.security.AllPermission;
};

// WebSphere system classes
grant codeBase "file:${was.install.root}/plugins/-" {
  permission java.security.AllPermission;
};
grant codeBase "file:${was.install.root}/lib/-" {
  permission java.security.AllPermission;
};
grant codeBase "file:${was.install.root}/classes/-" {
  permission java.security.AllPermission;
};

// Allow the WebSphere deploy tool all permissions
grant codeBase "file:${was.install.root}/deploytool/-" {
  permission java.security.AllPermission;
};

// Allow Channel Framework classes all permission
grant codeBase "file:${was.install.root}/installedChannels/-" {
  permission java.security.AllPermission;
};

// WebSphere optional runtime classes
grant codeBase "file:${was.install.root}/optionalLibraries/-" {
  permission java.security.AllPermission;
};
```

```
// ****************************************************************
// From here, Oracle Identity Manager application permission start
// ****************************************************************

// OIM codebase permissions
// Change Cell "XL_CELL" Value to the one in your installation
grant codeBase
  "file:${user.install.root}/installedApps/XL_CELL/Xellerate.ear/-" {

  // File permissions
  // Change Nodes "XL_NODE1" Value and Server "XL_SERVER_ON_NODE1" value
  // to the one in your installation
  permission java.io.FilePermission
    "${user.install.root}/temp/XL_NODE1/XL_SERVER_ON_NODE_1/-",
    "read,write,delete";
  // Need read, write, and delete permissions on $OIM_HOME/config folder
  // to read various config files, write the
  // xlconfig.xml.{0,1,2..} files upon re-encryption and delete
  // the last xlconfig.xml if the numbers go above 9.
  permission java.io.FilePermission "${XL.HomeDir}/config/-",
    "read, write, delete";
  permission java.io.FilePermission "${XL.HomeDir}/-", "read";
  // Need read, write, and delete permissions to generate adapter java
  // code, delete the .class file when the adapter is loaded into
  // the database
  permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
    "read,write,delete";
  // This is required by the connectors and connector installer
  permission java.io.FilePermission
    "${XL.HomeDir}/ConnectorDefaultDirectory/-", "read,write,delete";
  permission java.io.FilePermission "${XL.HomeDir}/connectorResources/-",
    "read,write,delete";
  // Must read Globalization resource bundle files for various
  // locales
  permission java.io.FilePermission "${XL.HomeDir}/customResources/-",
    "read";
  // Must read code from "JavaTasks", "ScheduleTask",
  // "ThirdParty", "EventHandlers" folder
  permission java.io.FilePermission "${XL.HomeDir}/EventHandlers/-",
    "read";
  permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-", "read";
  permission java.io.FilePermission "${XL.HomeDir}/ScheduleTask/-",
    "read";
  permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-", "read";
  // Required by the Generic Technology connector
  permission java.io.FilePermission "${XL.HomeDir}/GTC/-", "read";
  permission java.io.FilePermission "${java.home}/lib/-", "read";
  permission java.lang.RuntimePermission
    "accessClassInPackage.sun.security.action";
  // OIM server invokes the java compiler. You need "execute"
  // permissions on all files.
  permission java.io.FilePermission "<<ALL FILES>>", "execute";

  // Socket permissions
  // Basically we allow all permissions on non-privileged sockets
  // The multicast address should be the same as the one in
  // xlconfig.xml for javagroups communication
  permission java.net.SocketPermission "*:1024-",
    "connect,listen,resolve,accept";
```

```
// This IP address is a multicast address on which cluster
// communication takes place. Ensure that it is same as defined in
// xlConfig.xml
permission java.net.SocketPermission "231.145.165.117",
  "connect,accept,resolve";

// Property permissions
// Read and write OIM properties
// Read XL.*, java.* and log4j.* properties
permission java.util.PropertyPermission "XL.HomeDir", "read";
permission java.util.PropertyPermission "XL.*", "read";
permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
permission java.util.PropertyPermission "log4j.*", "read";
permission java.util.PropertyPermission "user.dir", "read";
permission java.util.PropertyPermission "file.encoding", "read";
permission java.util.PropertyPermission "java.class.path", "read";
permission java.util.PropertyPermission "java.ext.dirs", "read";
permission java.util.PropertyPermission "java.library.path", "read";

// Runtime permissions
// OIM server needs permissions to create its own class loader,
// get the class loader, modify threads and register shutdown
// hooks
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "getClassLoader";
permission java.lang.RuntimePermission "setContextClassLoader";
permission java.lang.RuntimePermission  "setFactory";
permission java.lang.RuntimePermission "modifyThread";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "shutdownHooks";
// OIM server needs runtime permissions to generate and load
// classes in the following packages. Also access the
// declared members of a class.
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.adapterGlue.ScheduleItemEvents";
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.dataobj.rulegenerators";
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.adapterGlue";
permission java.lang.RuntimePermission "accessDeclaredMembers";

// Reflection permissions
// Give permissions to access and invoke fields/methods from
// reflected classes.
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";

// Security permissions for OIM server
permission java.security.SecurityPermission "*";
permission java.security.SecurityPermission "insertProvider.IBMJCE";
permission javax.security.auth.AuthPermission "doAs";
permission javax.security.auth.AuthPermission "doPrivileged";
permission javax.security.auth.AuthPermission "getSubject";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext";
permission javax.security.auth.AuthPermission "getLoginConfiguration";
permission javax.security.auth.AuthPermission "setLoginConfiguration";
permission java.security.SecurityPermission
  "getProperty.policy.allowSystemProperty";
permission java.security.SecurityPermission
  "getProperty.login.config.url.1";
```

```
  permission javax.security.auth.AuthPermission
    "refreshLoginConfiguration";

  // SSL permission (for remote manager)
  permission javax.net.ssl.SSLPermission  "getSSLSessionContext";

  // Serializable permissions
  permission java.io.SerializablePermission "enableSubstitution";
};

// Grant AllPermission to nexaweb-common.jar
grant codeBase "file:${was.install.root}/lib/nexaweb-common.jar" {
  permission java.security.AllPermission;
};

// Grant AllPermission to wssec.jar
grant codeBase "file:${was.install.root}/lib/wssec.jar" {
  permission java.security.AllPermission;
};

// Nexaweb codebase permissions
// Change Cell "XL_CELL", Node "XL_NODE1" and Server "XL_SERVER_ON_NODE1"
// values to the one in your install
grant codeBase "file:${user.install.root}/installedApps/XL_CELL/Nexaweb.ear/-" {

  // File permissions
  permission java.io.FilePermission
    "${user.install.root}/temp/XL_NODE1/XL_SERVER_ON_NODE_1/-",
    "read,write,delete";
  permission java.io.FilePermission
    "${user.install.root}/installedApps/XL_CELL/Xellerate.ear/-", "read";
  permission java.io.FilePermission "${user.home}", "read, write";
  permission java.io.FilePermission
    "${user.install.root}/installedApps/XL_CELL/Nexaweb.ear/-", "read";
  permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
    "read,write,delete";
  permission java.io.FilePermission "<<ALL FILES>>", "execute";

  // Property permissions
  permission java.util.PropertyPermission "user.dir", "read";
  permission java.util.PropertyPermission "*", "read,write";

  // Runtime permissions
  // Nexaweb server needs permissions to create its own class loader,
  // get the class loader etc.
  permission java.lang.RuntimePermission "createClassLoader";
  permission java.lang.RuntimePermission "getClassLoader";
  permission java.lang.RuntimePermission "setContextClassLoader";
  permission java.lang.RuntimePermission  "setFactory";
  permission java.lang.RuntimePermission "shutdownHooks";
  // Nexaweb server security permissions to load the Cryptix
  // extension
  permission java.security.SecurityPermission "insertProvider.Cryptix";

  // Socket permissions
  // Permissions on all non-privileged ports.
  permission java.net.SocketPermission "*:1024-",
    "listen, connect, resolve";

  // Security permissions
```

```
  permission javax.security.auth.AuthPermission "doAs";
  permission javax.security.auth.AuthPermission "modifyPrincipals";
  permission javax.security.auth.AuthPermission "createLoginContext";
  permission java.lang.RuntimePermission "modifyThread";
  permission java.lang.RuntimePermission
    "accessClassInPackage.sun.security.action";
};

// The following are permissions given to codebase in the OIM server
// directory
grant codeBase "file:${XL.HomeDir}/-" {

  // File permissions
  permission java.io.FilePermission "${XL.HomeDir}/config/-", "read";
  permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-", "read";
  permission java.io.FilePermission "${XL.HomeDir}/ScheduleTasks/-",
    "read";
  permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-", "read";
  permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
    "read,write,delete";

  // Socket permissions
  permission java.net.SocketPermission "*:1024-",
    "connect,listen,resolve,accept";

  // Property permissions
  permission java.util.PropertyPermission "XL.HomeDir", "read";
  permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
  permission java.util.PropertyPermission "XL.*", "read";
  permission java.util.PropertyPermission "log4j.*", "read";
  permission java.util.PropertyPermission "user.dir", "read";

  // Security permissions
  permission javax.security.auth.AuthPermission "doAs";
  permission javax.security.auth.AuthPermission "modifyPrincipals";
  permission javax.security.auth.AuthPermission "createLoginContext";
  permission java.lang.RuntimePermission "modifyThread";
  permission java.lang.RuntimePermission
    "accessClassInPackage.sun.security.action";
};

// default permissions granted to all domains
grant {
  // "standard" properties that can be read by anyone
  permission java.util.PropertyPermission "java.version", "read";
  permission java.util.PropertyPermission "java.vendor", "read";
  permission java.util.PropertyPermission "java.vendor.url", "read";
  permission java.util.PropertyPermission "java.class.version", "read";
  permission java.util.PropertyPermission "os.name", "read";
  permission java.util.PropertyPermission "os.version", "read";
  permission java.util.PropertyPermission "os.arch", "read";
  permission java.util.PropertyPermission "file.separator", "read";
  permission java.util.PropertyPermission "path.separator", "read";
  permission java.util.PropertyPermission "line.separator", "read";
  permission java.util.PropertyPermission "java.specification.version", "read";
  permission java.util.PropertyPermission "java.specification.vendor", "read";
  permission java.util.PropertyPermission "java.specification.name", "read";
  permission java.util.PropertyPermission "java.vm.specification.version", "read";
  permission java.util.PropertyPermission "java.vm.specification.vendor", "read";
  permission java.util.PropertyPermission "java.vm.specification.name", "read";
```

```
  permission java.util.PropertyPermission "java.vm.version", "read";
  permission java.util.PropertyPermission "java.vm.vendor", "read";
  permission java.util.PropertyPermission "java.vm.name", "read";
  permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
  permission java.lang.RuntimePermission "accessDeclaredMembers";
  permission java.util.PropertyPermission "XL.*", "read";
  permission java.util.PropertyPermission "user.dir", "read";
  permission java.util.PropertyPermission "*", "read,write";
  permission java.lang.RuntimePermission "getClassLoader";
  permission java.lang.RuntimePermission "createClassLoader";
  permission java.lang.RuntimePermission "setContextClassLoader";
  permission java.util.PropertyPermission "nexaweb.logs", "read,write";
  permission java.lang.RuntimePermission "loadLibrary.*";
  permission java.lang.RuntimePermission "queuePrintJob";
  permission java.net.SocketPermission    "*", "connect";
  permission java.io.FilePermission   "<<ALL FILES>>", "read,write";
  permission java.lang.RuntimePermission   "modifyThreadGroup";
  permission javax.security.auth.AuthPermission "doAs";
  permission java.lang.RuntimePermission "modifyThread";
  permission com.ibm.websphere.security.WebSphereRuntimePermission
"AdminPermission";
};
```

B

Changing the Password of the xelsysadm User

The following sections describe the steps involved in changing the password for the xelsysadm administrative user for Oracle Identity Manager release 9.1.X deployed on IBM Websphere Application Server version 6.1.X.

B.1 Creating a Backup of the WebSphere Configuration and Oracle Identity Manager Database

Oracle recommends that you create a backup of the application server and database before changing the password for the xelsysadm user. Although a complete backup is recommended, the following backup is sufficient for this procedure:

> **Note:** When you create the backup, make sure that there is no user activity on the Oracle Identity Manager application and Websphere Application Server.

1. Create a backup of the WebSphere configuration by using *WAS_HOME*/profiles/*PROFILE_NAME*/bin/backupConfig.sh or backupConfig.cmd before starting this procedure. Changing password is a complicated process and you would need the WebSphere configuration backup to restore to the previous working state, if anything goes wrong. Refer to IBM documentation for more information on how to use the backupConfig utility. For clustered installation, create backup for all WebSphere profiles.
2. Create a backup of the database, specifically the USR table for the the row where `usr_login='XELSYSADM'`.

B.2 Changing the Password

To change the password of the xelsysadm user in IBM WebSphere Application Server 6.1.x:

1. Login to the WebSphere Admin Console and the Oracle Identity Manager Administrative and User Console in two different browser windows. For a

clustered installation of Oracle Identity Manager, make sure that all the node agents in XL_CELL are started, including the XL_MODEL_NODE.

2. Change the password for xelsysadm in the Administrative and USer Console. To do so:
   a. Login to Administrative and User Console as xelsysadm.
   b. Click **My Account**, and then click **Change Password**.
   c. Enter old and new passwords, and then click **OK** to change the password.

   Note: For a clustered installation of Oracle Identity Manager, shut down the `XL_JMS_CLUSTER` and `XL_CLUSTER` clusters.

3. Change the password in the WebSphere Admin Console for XLJMSLogin. To do so:

   Note: This step is not required if you are using WebSphere MQ for JMS messaging. Default installations of Oracle Identity Manager used WebSphere default JMS implementation.

   a. In the WebSphere Admin Console, click **Security**, **Secure Administration**, **Applications and Infrastructure**.
   b. On the right pane, click **Java Authentication and Authorization Service**, **J2C Authentication Data**, **XLJMSLogin**.
   c. Enter the new password and click **OK**.
   d. Save the password in the master configuration.
4. Change the password in the WebSphere Admin Console for standalone custom registry. To do so:
   a. In the WebSphere Admin Console, navigate to **Security**, **Secure Administration**, **Applications and infrastructure**, and **Standalone Custom Registry**.
   b. Enter the new password.
   c. Enter primary administrative user name as `xelsysadm`. The following warning message is displayed:

      ```
      The administrative user ID does not exist in the user repository.
      ```

   d. Ignore the warning and click **Save** to save the password in the master configuration.
5. Uninstall applications. To do so:
   a. In the WebSphere Admin Console, navigate to **Applications**, **Enterprise Applications**.
   b. Select **Xellerate and Nexaweb**, and click **Uninstall**.
   c. Click **Save** to save the password to the main configuration.

      For a clustered installation of Oracle Identity Manager, click **Preferences**, and select **Synchronize changes with Nodes** before saving.

6. Change the soap-client.properties. To do so, in the WebSphere installation, open the *WAS_HOME*/*PROFILE_NAME*/properties/soap.client.props file, and enter the new password for the com.ibm.SOAP.loginPassword property.

   For a clustered installation of Oracle Identity Manager, perform this step for WebSphere installations and profiles on all the nodes that are involved in XL_CELL.

7. Restart WebSphere Application Server.

   For a clustered installation of Oracle Identity Manager, restart Deployment Manager and Node Manager on all the nodes including XL_MODEL_NODE. Do not start WebSphere Application Servers in XL_CLUSTER and XL_JMS_CLUSTER.

8. Run the following utility to redeploy Oracle Identity Manager:

   - For UNIX

     OIM_HOME/setup/patch_websphere.sh *XELSYSADM_PASSWORD* *OIM_DB_PASSWORD*

   - For Microsoft Windows:

     OIM_HOME/setup/patch_websphere.cmd *XELSYSADM_PASSWORD* *OIM_DB_PASSWORD*

     Note: Provide the new password for xelsysadm to run the patch.

9. Restart WebSphere Application Server.

   For a clustered installation of Oracle Application Server, you can shutdown Node Manager on XL_MODEL_NODE. Start WebSphere Application Server in the XL_CLUSTER and XL_JMS_CLUSTER clusters.

10. Logout of the WebSphere Admin Console and relogin.

B.3 Rolling Back the Password Change

If a problem occurs while changing the password, then it is possible to rollback the changes by using the *WAS_HOME*/profiles/*PROFILE_NAME*/bin/restoreConfig.sh or restoreConfig.cmd script. Refer to IBM documentation for more information on how to use this utility.

You must also restore the USR table from the backup. For example, restore the USR table for the row where usr_login='XELSYSADM'.

C

Using IBM WebSphere Application Server MQ as JMS Provider

This appendix provides an overview for using WebSphere MQ as JMS provider for Oracle Identity Manager. For detailed information you have to refer to WebSphere and WebSphere MQ documentation.

Using WebSphere MQ as JMS provider for Oracle Identity Manager involves the following steps:

- Creating a Backup of the WebSphere 6.1 Configuration
- Preparing WebSphere MQ
- Uninstalling Applications
- Removing Resources for Default Messaging
- Changing the xlJMSLogin Credentials
- Creating WebSphere MQ Resources
- Changing Deployment Descriptors
- Restarting IBM WebSphere Application Server
- Running the patch_websphere Patch
- Restarting WebSphere Application Server
-

C.1 Creating a Backup of the WebSphere 6.1 Configuration

Oracle recommends that you create a backup of the WebSphere configuration for all the WebSphere profiles involved in the installation of Oracle Identity Manager. You need the WebSphere configuration backup to restore to the previous working state, if anything goes wrong. Refer to IBM documentation on how to use the `backupConfig` and `restoreConfig` utilities for creating backup and restoring the WebSphere configuration respectively.

To create a backup of the WebSphere configuration for all the profiles in WebSphere 6.1, run the *`WAS_HOME`*`/profiles/`*`PROFILE_NAME`*`/bin/backupConfig.sh` or `backupConfig.cmd` script.

In addition, create a backup of the *`OIM_HOME`* directory before starting the procedure described in this appendix.

C.2 Preparing WebSphere MQ

Install MQ in one or more computers. For example, for failover, install MQ in one computer with hardware-based failover, or install MQ in multiple computers and create a clustered queue manager.

Create six separate JMS queues in the Queue Manager by naming the queues appropriately. For example, create queues named xlQueue, xlAuditQueue, xlAttestationQueue, xlReconQueue, xlProcessQueue, and xlErrorQueue. xlErrorQueue is intended to be used as a dead letter queue for all other five queues.

C.3 Uninstalling Applications

Uninstall Oracle Identity Manager applications already deployed from the IBM application server for integrating WebSphere MQ with Oracle Identity Manager. To do so:

1. In the WebSphere Admin Console, navigate to **Applications**, and then to **Enterprise Applications**.
2. Select **Xellerate**, and then select **Nexaweb**.
3. Click **Uninstall**.

C.4 Removing Resources for Default Messaging

To remove resource for default messaging:

1. In the WebSphere Admin Console, navigate to **Resources**, **JMS**, **Queue Connection Factories**.
2. Set the scope to the Cell Level for clustered and to the server level for nonclustered installations.
3. Select **xlConnectionFactory**, and then click **Delete** to remove it.
4. Navigate to **Resources**, **JMS**, **Queues**.
5. Set the scope to the Cell Level for clustered and to the server level for nonclustered installations.
6. Select all the queues that start with xl, and then click **Delete**.
7. Navigate to **Resources**, **JMS**, **Activation Specification**.
8. Set the scope to the Cell Level for clustered and to the server level for nonclustered installations.
9. Select all the activation specifications, and then click **Delete** to remove all.
10. Navigate to Service **Integration**, and then to **Buses**.
11. Select **XellerateBus**, and then click **Delete** to remove.
12. Click Save to save the changes in the main configuration.

Note: For a clustered installation of Oracle Identity Manager, make sure to click **Preferences**, and select **Synchronize changes with Nodes** before clicking **Save**.

C.5 Changing the xlJMSLogin Credentials

To change the xlJMSLogic credentials:

1. Navigate to **Security**, **Secure administration, applications and infrastructure**, **Java Authentication and Authorization Service (Under Authentication)**, **J2C authentication data**.
2. Click **XLJMSLogin**, and change the User ID and Password to the WebSphere MQ user name and password.

C.6 Creating WebSphere MQ Resources

To create WebSphere MQ resources:

1. Create queue connection factory. To do so:
   a. In the WebSphere Admin Console, navigate to **Resources**, **JMS**, **Queue Connection Factories**.
   b. Set the scope to the Cell Level for clustered and to the server level for nonclustered installations.
   c. Click **New**, and select **WebSphere MQ messaging provider**, and then click **OK**.
   d. For Name and JNDI name, enter **xlConnectionFactory**.
   e. Enter the other required information related to WebSphere MQ.
2. Create queue references on WebSphere:
   a. In the WebSphere Admin Console, navigate to **Resources**, **JMS**, **Queues**.
   b. Set the scope to the Cell Level for clustered and to the server level for nonclustered installations.
   c. Click **New**, and select **WebSphere MQ messaging provider**, and then click **OK**.
   d. Enter Name as **xlQueue**, JNDI name as **queue/xlQueue**, Base queue name as the name of the appropriate queue on Websphere MQ.
   e. Create six new queues with the following JNDI names:

      queue/xlQueue, queue/xlReconQueue, queue/xlAuditQueue, queue/xlAttestationQueue, queue/xlProcessQueue, and queue/xlErrorQueue
3. Create listener ports. To do so, in the WebSphere Admin Console, navigate to **Servers**, **Application Servers**, ***SERVER_NAME***, **Messaging**, **Message Listener Service**, **Listener Ports**. Then create the following listener ports:
   - MessageHandlerMDB_JMSPort:
     - Name: **MessageHandlerMDB_JMSPort**
     - Connection factory JNDI name: **xlConnectionFactory**
     - Destination JNDI name: **queue/xlQueue**
   - ReconMessageHandlerMDB_JMSPort:
     - Name: **ReconMessageHandlerMDB_JMSPort**
     - Connection factory JNDI name: **xlConnectionFactory**
     - Destination JNDI name: **queue/xlReconQueue**

- AuditMessageHandlerMDB_JMSPort:
  - Name: **AuditMessageHandlerMDB_JMSPort**
  - Connection factory JNDI name: **xlConnectionFactory**
  - Destination JNDI name: **queue/xlAuditQueue**
- AttestationMessageHandlerMDB_JMSPort:
  - Name: **AttestationMessageHandlerMDB_JMSPort**
  - Connection factory JNDI name: **xlConnectionFactory**
  - Destination JNDI name: **queue/xlAttestationQueue**
- ProcessMessageHandlerMDB_JMSPort:
  - Name: **ProcessMessageHandlerMDB_JMSPort**
  - Connection factory JNDI name: **xlConnectionFactory**
  - Destination JNDI name: **queue/xlProcessQueue**

Note: For a clustered installation of Oracle Identity Manager, the step for creating listener ports must be repeated for all the servers in `XL_CLUSTER`.

C.7 Changing Deployment Descriptors

To make the message driven beans listen to MQ destinations, change the deployment descriptors. To do so:

1. Open the *`OIM_HOME`*`/DDTemplates/BO/ibm-ejb-jar-bnd.xmi` file.
2. Replace all occurrences of activationSpecJndiName with **listenerInputPortName**.
3. Replace xlQueueSpec with **MessageHandlerMDB_JMSPort**.
4. Replace xlReconQueueSpec with **ReconMessageHandlerMDB_JMSPort**.
5. Replace xlAuditQueueSpec with **AuditMessageHandlerMDB_JMSPort**.
6. Replace xlAttestationQueueSpec with **AttestationMessageHandlerMDB_JMSPort**.
7. Replace xlProcessQueueSpec with **ProcessMessageHandlerMDB_JMSPort**.
8. Save the ibm-ejb-jar-bnd.xmi file.

Note: For a clustered installation of Oracle Identity Manager, copy the ibm-ejb-jar-bnd.xmi file to all the nodes on which Oracle Identity Manager is deployed.

C.8 Restarting IBM WebSphere Application Server

Restart WebSphere Application Server. For a clustered installation of Oracle Identity Manager, restart all the application servers as well as the Deployment Manager.

C.9 Running the patch_websphere Patch

Run the following patch utility to deploy Oracle Identity Manager with MQ integration:

- For UNIX:

  OIM_HOME/setup/patch_websphere.sh *XELSYSADM_PASSWD OIM_DB_PASSWD*

- For Microsoft Windows:

  OIM_HOME/setup/patch_websphere.cmd *XELSYSADM_PASSWD OIM_DB_PASSWD*

C.10 Restarting WebSphere Application Server

Restart WebSphere Application Server. For a clustered installation of Oracle Identity Manager, restart all the application servers as well as the Deployment Manager.

C.11 Rolling Back MQ Configuration

If required, then restore *OIM_HOME* and rollback the changes to IBM WebSphere Application Server by using the *WAS_HOME*/profiles/*PROFILE_NAME*/bin/restoreConfig.sh or restoreConfig.cmd script. Refer to IBM documentation for more information on how to use this utility.

Index

J

K

L

N

O

P

R

S

T

W

X