

Oracle® Role Manager

Installation Guide

Release 10g (10.1.4)

E12026-05

February 2009

Oracle Role Manager Installation Guide Release 10g (10.1.4)

E12026-05

Copyright © 2008, 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Prakash Hulikere

Contributing Author: Carla Fabrizio

Contributor: Miles Chaston, Ashish Chugh, April Escamilla, Bennett Falk, Seth Klein, Richard Mehler, Devender Sharma

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	x
Conventions	x
1 Overview of Oracle Role Manager Installation	
1.1 Role Manager Installation Methods	1-1
1.1.1 Interactive Installation Methods	1-1
1.1.2 Automated Installation Methods Using Response Files	1-1
1.2 Role Manager Installation	1-2
1.3 Installation Considerations	1-2
1.3.1 Hardware and Software Considerations	1-3
1.3.2 Multiple Oracle Homes	1-3
1.4 About the Single Sign-On Configuration with Oracle Role Manager	1-3
2 Oracle Role Manager Installation Requirements	
2.1 Host Requirements for Role Manager Components	2-1
2.1.1 Role Manager Application Server Host Requirements	2-1
2.1.2 Database Server Host Requirements	2-1
2.2 Planning Your Installation	2-1
2.2.1 Installation Worksheet	2-2
3 Installing Oracle Role Manager	
3.1 Before You Start	3-1
3.2 Database Setup	3-1
3.2.1 Creating the Role Manager Tablespaces	3-2
3.2.2 Creating the Role Manager Users	3-3
3.3 Installing Role Manager	3-3
3.4 Performing a Silent Installation Using a Response File	3-6
4 Application Server Configuration	
4.1 Before You Configure the Application Server	4-1
4.2 Configuring WebLogic Server	4-1

4.2.1	Configuring Oracle WebLogic Server in a Nonclustered Mode.....	4-1
4.2.1.1	Configuring WebLogic Server	4-2
4.2.2	Configuring Oracle WebLogic Server in a Clustered Mode.....	4-5
4.2.2.1	About Oracle WebLogic Server Clusters	4-5
4.2.2.2	Configuring WebLogic 10.3 Clusters.....	4-5
4.2.2.3	Configuring Apache Failover Proxy.....	4-14
4.3	Configuring JBoss	4-15
4.3.1	Encrypting the Role Manager Database Password.....	4-17
4.3.2	Configuring Data Upload Size Limit	4-18
4.4	Configuring IBM WebSphere.....	4-18
4.4.1	Creating a Non-Administrative Server for Deploying Oracle Role Manager	4-20
4.4.2	Configuring WebSphere to Use a Non-Default HTTP Port	4-20
4.4.3	Configuring JDBC Providers.....	4-20
4.4.4	Reconfiguring JDBC Providers	4-21
4.4.5	Creating the Role Manager Database Credentials	4-22
4.4.6	Configuring the Non-XA Data Source.....	4-22
4.4.7	Configuring the Transaction (XA) Data Source	4-23
4.4.8	Configuring the JMS messaging buses	4-24
4.4.9	Configuring Bus Destinations.....	4-25
4.4.10	Configuring JMS Queue Connection Factories	4-25
4.4.11	Configuring the JMS Topic Connection Factory	4-26
4.4.12	Configuring JMS Queues.....	4-26
4.4.13	Configuring the JMS Notification Topic.....	4-27
4.4.14	Configuring JMS Activation Specifications	4-27
4.4.15	Securing the WebSphere Installation/Console	4-29
4.4.16	Creating a Custom User.....	4-29
4.4.17	Creating Alias for Custom User	4-30
4.4.18	Configuring Connection Factory Authentication	4-30
4.4.19	Configuring Activation Specification Authentication.....	4-30
4.4.20	Securing the Message Bus	4-31
4.4.21	Configuring Data Upload Size Limit.....	4-31
4.4.22	Increasing the Transaction Timeout.....	4-32
4.4.23	Deploying Role Manager Server	4-32
4.4.24	Deploying the Role Manager Web Application	4-33

5 Loading Data

5.1	Loading Standard and Sample Data	5-1
5.2	Manual Data Model Deployment.....	5-2

6 Removing Oracle Role Manager Software

6.1	Removing Oracle Role Manager Software	6-1
6.2	Removing the Oracle Role Manager Database	6-2

A Manual Configuration of WebLogic Server

A.1	Overview	A-1
A.1.1	Creating a New Domain	A-1

A.1.2	Configuring Memory options	A-2
A.1.3	Starting WebLogic Server	A-3
A.1.4	Configuring Machines	A-4
A.1.5	Configuring Servers	A-4
A.1.6	Setting Up Commons Logging	A-5
A.1.7	Configuring JDBC Data Sources.....	A-6
A.1.8	Configuring JMS Messaging Resources	A-7
A.1.9	Configuring JMS Module Subdeployment	A-8
A.1.10	Configuring the JMS Connection Factory	A-8
A.1.11	Configuring a Notification Topic	A-9
A.1.12	Configuring Queues	A-9
A.1.13	Configuring Data Upload Size Limit	A-10
A.1.14	Creating the Oracle Role Manager User.....	A-11
A.1.15	Deploying Role Manager.....	A-11

Index

List of Tables

2-1	Installation Worksheet	2-2
4-1	WebLogic-Based Oracle Role Manager Cluster Host Computers	4-5

Preface

Oracle Role Manager Installation Guide explains how to prepare for, install, and configure Oracle Role Manager (Role Manager). It provides specific instructions for the operating system and Oracle software technology components that Role Manager requires.

Audience

This document is intended for Oracle database administrators (DBAs) and system administrators, and those who are involved in the installation of Oracle Role Manager and its related components.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

For more information, refer to the following documents:

- *Oracle Role Manager Release Notes*
- *Oracle Role Manager Administrator's Guide*
- *Oracle Role Manager User's Guide*
- *Oracle Role Manager Developer's Guide*
- *Oracle Role Manager Java API Reference*
- *Oracle Role Manager Integration Guide*

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.
<i>italic</i>	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.

Overview of Oracle Role Manager Installation

Oracle Role Manager (Role Manager) is an enterprise-class application for managing business and organizational relationships, roles and entitlements. An application for role lifecycle management and an authoritative repository for roles across the IT infrastructure, it drives automation of role-based provisioning and access control. Role Manager is a component of Oracle's Identity Management and Oracle Fusion Middleware.

This chapter provides an overview of the Role Manager installation process. This chapter includes the following sections:

- [Role Manager Installation Methods](#)
- [Role Manager Installation](#)
- [Installation Considerations](#)
- [About the Single Sign-On Configuration with Oracle Role Manager](#)

1.1 Role Manager Installation Methods

You can choose different installation methods to install Role Manager, as follows:

- [Interactive Installation Methods](#)
- [Automated Installation Methods Using Response Files](#)

1.1.1 Interactive Installation Methods

When you use the interactive method to install Role Manager, Oracle Universal Installer displays a series of screens that enable you to specify all of the required information to install the Role Manager software.

1.1.2 Automated Installation Methods Using Response Files

This installation method is for experienced users. If you are installing Role Manager for the first time, it is recommended that you run the Oracle Universal Installer using the interactive installation method as described in "[Installing Oracle Role Manager](#)" on page 3-1.

Role Manager provides a response file template for installation (`orm.rsp`). The response template file can be found in the `<ORM_installation-Media>Disk1/stage/response` directory on the Role Manager installation media.

When you start Oracle Universal Installer and specify a response file, you can automate all of the Role Manager installation. These automated installation methods are useful if you need to perform multiple installations on similarly configured systems.

For Role Manager, Oracle Universal Installer can run in silent (non-interactive) mode. For silent mode, specify both the `-silent` and `-responseFile` options followed by the path of the response file on the command line when you invoke Oracle Universal Installer. For example:

```
setup.exe -silent -responseFile <Absolute Path of response file>
```

Oracle Universal Installer runs in silent mode if you use a response file that specifies all required information. None of the Oracle Universal Installer screens are displayed, and the logs are created under the `oraInventory` location, similar to interactive mode installation.

Prepare the response file by entering values for all parameters that are missing, and then save the file. Do not edit any values in the second part of either response file.

See "[Performing a Silent Installation Using a Response File](#)" on page 6 for information about performing an Role Manager silent installation.

Note: The basic installation is not supported in silent mode. Silent installation is only supported for the advanced installation.

1.2 Role Manager Installation

The Role Manager installation consists of two options:

- **Install Software and Configure**—This is the recommended way to install Oracle Manager. This option requires that two empty database schema/users are already created, and requires connectivity to database to load the data model for a standard installation.
- **Install Software Only**—This option provides the opportunity to copy the software onto the file system and then later load the data model after customizations are put into place. This is normally done after being familiar with the product in its standard form and having identified all of the modeling changes for your business needs.

After you check the requirements described in "[Installation Considerations](#)" on page 1-2, the general steps to install Role Manager include these tasks:

1. Run Oracle Universal Installer to perform Role Manager installation and configuration.
2. Configure your application server with Role Manager.
3. Load the sample data for Role Manager.

1.3 Installation Considerations

This section contains information that you should consider before deciding how to install this product. It includes the following topics:

- [Hardware and Software Considerations](#)
- [Multiple Oracle Homes](#)

1.3.1 Hardware and Software Considerations

The platform-specific hardware and software requirements included in this installation guide were current at the time this guide was published. However, because new platforms and operating system versions might be certified after this guide is published, review the certification matrix on the *OracleMetaLink* Web site for the most up-to-date list of certified hardware platforms and operating system versions. For example, the *OracleMetaLink* Web site is available at:

<http://metalink.oracle.com>

If you do not have a current Oracle Support Services contract, then for example, you can access the same information at:

<http://www.oracle.com/technology/support/metalink/content.html>

Refer to the *Oracle Role Manager Release Notes* for detailed system requirements and supported platforms.

1.3.2 Multiple Oracle Homes

This product supports multiple Oracle homes. You can install this release of the software more than once on the same system, in different Oracle home directories.

1.4 About the Single Sign-On Configuration with Oracle Role Manager

The configuration of Oracle Access Manager with Oracle Role Manager provides a secure web-based infrastructure for role management for all customer applications and processes. Oracle Access Manager integrates identity and access management across Oracle Role Manager, enterprise resources, and other domains deployed on eBusiness networks. Oracle Access Manager provides the foundation for managing the identities of customers, partners, and employees across internet applications. These user identities are combined with security policies for protected web interaction.

For more information about Oracle Role Manager single sign-on, refer to the "Oracle Role Manager Administrator's Guide".

Oracle Role Manager Installation Requirements

This chapter describes Oracle Role Manager (Role Manager) installation requirements. This chapter includes the following sections:

- [Host Requirements for Role Manager Components](#)
- [Planning Your Installation](#)

2.1 Host Requirements for Role Manager Components

You must obtain enterprise versions of application server software and database software complete with valid licenses. Role Manager does not include the application server or database software.

The Role Manager installation program may conflict with other installed applications, utilities, or drivers. Try to remove all non-essential software and drivers from the installation computer before loading Role Manager.

Important: Always check the *Oracle Role Manager Release Notes* for the requirements and supported configurations specific to each version. The information in this guide applies to the Oracle Role Manager 10.1.x versions.

2.1.1 Role Manager Application Server Host Requirements

Refer to the *Oracle Role Manager Release Notes* for the specific application server host requirements.

2.1.2 Database Server Host Requirements

Refer to the Oracle Database documentation for the specific database host requirements.

2.2 Planning Your Installation

Before installing Role Manager, you must read "[Host Requirements for Role Manager Components](#)" on page 2-1 and "[Installation Worksheet](#)" on page 2-2 to help plan your installation.

Because the Database Administrator (DBA), System Administrator, and IT Developer typically handle tasks specific to their specific areas of expertise, you should share Role Manager installation information among your team members.

2.2.1 Installation Worksheet

The Installation Worksheet table helps you identify configuration attributes you need before starting the Role Manager installation. Print this worksheet and use it to take notes as you go through your installation. Use the User Selection column to fill in information specific to your installation:

Table 2-1 Installation Worksheet

Item	User Selection
Base directory for installing Role Manager.	
Name or IP address of the computer where the Role Manager database is installed.	
TCP listener port number for the database..	
Service name of the database for your installation.	
User name and password of the SYSTEM user account for access to the database.	
Name or IP address of the application server computer.	
TCP listener port number for the application server.	

Installing Oracle Role Manager

This chapter includes the major steps required to install Oracle Role Manager (Role Manager).

This chapter includes the following sections:

- [Before You Start](#)
- [Database Setup](#)
- [Installing Role Manager](#)
- [Performing a Silent Installation Using a Response File](#)

3.1 Before You Start

Before you begin the Role Manager installation, you must create a Role Manager database user (owner) and Role Manager application user.

Before performing the procedures in this chapter, ensure the following:

- The installation computer has network access to the database server host.
- You have the necessary information from the [Installation Worksheet](#) on page 2-2.
- For UNIX-based systems—It is recommended that you create a special user account, such as `orm`, and set its home directory to the directory you plan to use for installation. You may want to have all dependent applications (such as JBoss and WebSphere) participate in the same group.

3.2 Database Setup

Before installing Role Manager, you need to create the database owner and application user schemas on the database used for Role Manager. Database owner is the user with permissions to change the schema, but the application user does not have permissions to change the schema. It is recommended that you use the scripts provided on the installation media following the procedures in this section. These steps, described in this section, are normally performed by a database administrator on the Oracle database host.

Before continuing, ensure that you have met the following requirements:

- The Oracle service and TNSListener are running.
- You have the Oracle `SYSTEM` account user name and password.
- You have the Oracle service name (instance).

- Optional: You have OS-level permission to edit the `init.ora` file to configure the Oracle rollback segments created as part of the Role Manager installation.

3.2.1 Creating the Role Manager Tablespaces

Before the Role Manager data model can be deployed, either by the Role Manager installer or manually at the command line, the tablespaces for Role Manager must exist.

Your policies may require that the scripts referenced in this section be run directly on the Oracle database server by a database administrator.

The provided tablespace creation script needs to be modified if your organization requires different extent and growth options. If you instead prefer to use your own tablespace creation script, the Role Manager user creation scripts expect three tablespaces, one for DATA pages named `ORM_DATA`, one for INDEX pages named `ORM_INDEX`, and one for TEMP space.

To create the Role Manager tablespaces:

1. From the installation media, copy the `create-tablespace.sql` script from the `samples/sqlscripts/oracle` directory to a temporary location.
2. Optionally, in the `create-tablespace.sql` file, edit the path to the log directory you want to use to save messages created by this script. For example:

```
set echo on;
spool <new_log_path>/create-tablespace.log
```
3. Optionally, in the same file, modify the tablespace definitions to meet your specific configuration requirements.

Note: If you modify the actual tablespace names in the `create-tablespace.sql` script in any way, you must also modify the `create-schema-owner.sql` and `create-app-user.sql` scripts, as appropriate, to accommodate the changed tablespace names.

4. Using `sqlplus` or a similar utility, run the `create-tablespace.sql` script to create the tablespaces for Role Manager database table data, index, temporary data, and rollback segments. For example:

```
sqlplus system/<system_pw>@<db_service> @create-tablespace <data_dir>/ORM_DATA
<index_dir>/ORM_INDEX <temp_dir>/ORM_TEMP
<undo_dir>/ORM_UNDO
```

Note: The data and index table spaces must be named `ORM_DATA` and `ORM_INDEX` respectively.

5. Review the contents of the `create-tablespace.log` file to verify there were no error messages.

If there are errors, ensure that the Oracle database paths you specified in the command are valid.

6. Optionally, configure rollback segments.

Rollback segments are used to save data in transactions before data is committed to the database. To bring the rollback segments online automatically every time the Oracle instance is restarted, you must update the init.ora file by adding the following line

```
ROLLBACK_SEGMENTS = (ORM_1, ORM_2, ORM_3, ORM_4)
```

3.2.2 Creating the Role Manager Users

Before creating the Role Manager users, ensure that the tablespaces used for Role Manager have been created.

To create the Role Manager database users:

1. From the installation media, copy the following scripts from the samples/sqlscripts/oracle directory to a temporary location:

```
create-app-user.sql
create-schema-owner.sql
```

2. As the Oracle `SYSTEM` user, using sqlplus or a similar utility, create the Role Manager database owner by running the create-schema-owner.sql script as follows:

```
sqlplus system/[system_pw]@[db_service] @create-schema-owner [owner_username]
```

Enter the password at the prompt and make note of username and password values, because you need them when running the Role Manager installer.

If you have changed tablespace names, ensure to use the same names as those defined in the create-tablespace.sql file.

Note: Errors in the console in the form "does not exist" are normal the first time this script and the following script are run.

3. Create the application user for Role Manager by running the create-app-user.sql script as follows:

```
sqlplus system/[system_pw]@[db_service] @create-app-user [app_username]
```

Enter the password at the prompt and make note of username and password values, because you need them when running the Role Manager installer.

Role Manager uses two schema/users, one as the owner and the other as the user of the application. This is done for security reasons, ensuring that schema changes can be made only by the owner. As part of the configuration process, the installer creates all of the synonyms required so that the Role Manager application user can invoke data changes.

Note: These users/schemas must already exist and name and password values must match what was used when they were created. Refer to "[Creating the Role Manager Users](#)" for information.

3.3 Installing Role Manager

In this part of the installation, you launch the installer and configure Role Manager with your environment.

To perform the Role Manager installation:

1. Ensure that the drive or directory containing the Role Manager installation media is accessible from the installation computer.
2. Run Oracle Universal Installer (OUI) to install Role Manager.

For Windows systems:

- Locate the directory containing the Role Manager installation files for Windows.
- Double-click `setup.exe`.

For UNIX-based systems:

- Change directory to the location containing the Role Manager installation files for your operating system.
- As the software owner account that owns the current `ORACLE_HOME` environment, start the installer with the following command:

```
./runInstaller
```

Note: If you do not know the account to use, contact your system administrator or DBA for information specific to your environment.

3. On the Welcome page, click **Next**.
4. On the Specify File Location page:
 - a. Ensure that the source path is pointing to the Role Manager installation media, for example:

```
C:\stage\products.xml
```
 - b. If you already have any oracle products on the installation computer, type a new unique identifier that Oracle can use for inventory purposes, such as `orm`.
 - c. Change the destination path to the location on the file system where you want to install the Role Manager software.

Note: The destination must be an empty directory. The installer creates the directory you specify if it does not already exist.

5. Choose one of the following installation options, then click **Next** to continue.
 - **Install Software and Configure**

This option installs the Role Manager software and then configures the database with the primordial data model. It also provides additional options to include the standard data model used by the Role Manager UI. If you do not yet have a customized data model, select this option.
 - **Install Software Only**

This option copies the Role Manager files to the specified installation location. It does not load any configuration or deploy the models required to use the Role Manager UI. This option is intended for manual deployments of customized models. Choosing this selection skips to the Summary page of the installer.

6. Select the configuration options you want, then click **Next** to continue.
 - **Primordial Data Model**
The core model used by the Role Manager system components.
 - **Standard Data Model**
This is required to load the standard configurations to Oracle Role Manager system.
7. Set the database connection values in the Database Connect String as follows:
 - a. For a single database host instance, provide the connection string as follows:

```
<Database-server host name>:<database server port number>:<Database service name>
```
 - b. For a real application cluster (RAC) database instance, provide the connection string as follows:

```
<Database-server instance1 host name>:<database server instance1 port number>^<Databaseserver instance2 host name>:<database server instance2 port number>@<Database service name>
```
8. Set the values needed to configure the Role Manager database tables as described below.
 - a. In the **Database Owner** field, type the name to use for the Role Manager owner schema/user.
 - b. In the **Database Owner Password** field, type the password to use for the Role Manager owner schema/user.
 - c. In the **Application User** field, type the name to use for the Role Manager application user schema.
 - d. In the **Application User Password** field, type the password to use for the Role Manager application user schema.
 - e. Click **Next** to continue.
9. Create the administrative account for Role Manager as follows:
 - a. Type a name to use as the Role Manager Administrator user ID.
 - b. Type a password for the Role Manager Administrator.
 - c. Retype the password in the Confirm Password field, then click **Next** to continue.

Oracle Universal Installer checks the system to verify that it is configured correctly to run Oracle software. If you have completed all of the preinstallation steps in this guide, all of the checks should pass.

If a check fails, then review the cause of the failure listed for that check on the screen. If possible, rectify the problem and rerun the check. Alternatively, if you are satisfied that your system meets the requirements, then you can select the check box for the failed check to manually verify the requirement.

10. On the installation Summary page, review the installation summary information. After reviewing this installation information, click **Install** to begin the installation procedure.

11. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file can be found in the `cfgtoollogs/oui` directory, in the following location:

For Windows systems:

```
%SYSTEMDRIVE%\Program Files\Oracle\Inventory\oraInventory
```

For UNIX-based systems:

If your computer already has the `oraInst.loc` file at the `"/etc"` location, then `oraInventory` is created at that location. This is depicted in the following example:

```
cat /etc/oraInst.loc
inventory_loc=/home/spatra/oraInventory123
```

If your computer is not having the `oraInst.loc` file at the `"/etc"` location, then `oraInventory` is created by default at `$HOME/oraInventory`, where `$HOME` is the user home.

Note: When `runInstaller.sh` (linux or aix) or `setup.exe` (windows) is executed, it displays the log location.

12. After the installation completes, click **Exit**, then click **Yes** to confirm.

3.4 Performing a Silent Installation Using a Response File

Follow these brief steps to perform a silent installation using a response file:

1. Ensure that all prerequisites are met for the installation of Role Manager.
2. Prepare the Role Manager response file. A template response file can be found with the Role Manager installation media at `stage/Response/orm.rsp`.

Prepare the response file by entering values in the file for all parameters, then save the file.

3. Invoke Oracle Universal Installer using the following options:

For UNIX-based systems:

```
./runInstaller -silent -responseFile <path_to_rsp>
```

For Windows systems:

```
setup.exe -silent -responseFile <path_to_rsp>
```

In this example:

`Path_to_rsp` identifies the full path of the response file.

`-silent` runs Oracle Universal Installer in silent mode and suppresses the Welcome window.

For general information about these options and about how to complete an installation using these response files, see the platform specific Oracle Database installation guides and *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux* and "Installing Oracle Products" in *Oracle Universal Installer and OPatch User's Guide* for more information about installing and using response files.

Application Server Configuration

This chapter includes the steps required to configure the application server to run the Oracle Role Manager (Role Manager) server and Web application.

This chapter includes the following sections:

- [Before You Configure the Application Server](#)
- [Configuring WebLogic Server](#)
- [Configuring JBoss](#)
- [Configuring IBM WebSphere](#)

4.1 Before You Configure the Application Server

Role Manager is intended to be deployed on only one server platform per installation. The server platform can be one of the following:

- Oracle WebLogic Server
- JBoss
- IBM WebSphere

The procedures in this chapter assume the following:

- The application server system has network access to the database server host.
- The Role Manager software is accessible by the application server system.
- You know the application server's listener port and host name.
- If running on WebSphere, a server, cell, and node to use for Role Manager have been created and configured.

4.2 Configuring WebLogic Server

You can configure WebLogic server in a clustered mode and a nonclustered mode. This section includes the following topics:

- [Configuring Oracle WebLogic Server in a Nonclustered Mode](#)
- [Configuring Oracle WebLogic Server in a Clustered Mode](#)

4.2.1 Configuring Oracle WebLogic Server in a Nonclustered Mode

You can configure the WebLogic server either manually or automatically, following an extension template. This section provides the information about automated

configuration of WebLogic server. If you want to configure the WebLogic server manually, refer to [Appendix A](#).

Note: Before you run the automated configuration of WebLogic server, ensure that the WebLogic server is installed and the node manager is up and running. You can start the node manager by running the `BEA_HOME/wlserver_10.3/server/bin/startNodeManager.sh` script for Linux.

`BEA_HOME/wlserver_10.3/server/bin/startNodeManager.cmd` script for Microsoft Windows.

You must configure WebLogic server in SSL mode to operate in a secure environment. For information about configuring SSL for WebLogic server, refer to the following URL:

<http://e-docs.bea.com/wls/docs103/secmanage/ssl.html>

4.2.1.1 Configuring WebLogic Server

To perform the template based configuration of WebLogic server:

1. Run the configuration wizard in WebLogic server directory:
`BEA_HOME\wlserver_10.3\common\bin\config.exe` or `config.sh`
2. When the configuration wizard is displayed, select **Create a new WebLogic Domain** and click **Next**.
3. Select **Base this domain on an existing templateORM** and go to:
`ORM_HOME/weblogic/templates/10.3/orm_createdomain_template_103.jar`
4. Click **Next**.
5. In the Configure Administrator Username and Password window, type **User Name** and **Password** and then click **Next**.
6. Configure server start mode and JDK by performing the following steps:
 - a. On the left side of the window, select either **Development Mode** or **Production Mode**, based on your server configuration.
 - b. On the right side of the window, select **Oracle SDK** and click **Next**.
7. A message is displayed asking whether you want to customize any of the options mentioned. Select **Yes**.
8. Click **Next**.
9. In the Configure RDBMS Security Store Database window, select **I don't want to change anything here** and click **Next**.
10. In the Configure Administration Server window, set the Listen Address to a value appropriate to your setup such as, LocalHost, IP Address, DNS equivalent and Listen Port and then click **Next**.
11. In the Configure Managed Servers window, set the Listen Address to a value appropriate to your setup such as, LocalHost, IP Address, DNS equivalent and Listen Port and then click **Next**.

12. In the Configure Clusters window, click **Next**.
13. In the Configure Machines window:
 - for UNIX machine, click the **UNIX machine** tab, the Oracle Role Manager machine name is auto populated. Click **Next**.
 - for Windows machine, click the **UNIX machine** tab and delete the existing Oracle Role Manager machine name, **ormMachine**. On the **Machine** tab, click **Add** and then type Oracle Role Manager machine name, Node manager listen address, and Node manager listen port, and then click **Next**.
14. In the Assign servers to machines window, select **AdminServer** on the left window, click the right arrow and select **ormMachine** on the right window, and then click **Next**.
15. In the Configure Data Sources window, in both the **ORM XA Data Source** tab and the **ORM Data Source** tab, type the DBMS details such as **Name**, **Host**, **Port**, **User Name**, and **Password** and click **Next**.

Note: If you are using RAC database, provide the following string while creating the data source:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1-vip)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2-vip)
(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=orcl.us.oracle.com)))
```

16. In the Review WebLogic Domain window, verify the details and click **Next**.
17. Click **Create**. The domain is created and the following are configured automatically:
 - a. Admin server is created.
 - b. Managed server for Oracle Role Manager is created.
 - c. Non-XA Data Source, Oracle Role Manager Data Source is created.
 - d. XA Data Source, Oracle Role Manager XA Data Source is created.
 - e. JMS Server, Oracle Role Manager JMSServer is created.
 - f. JMS Module, Oracle Role Manager JMSModule is created.
 - g. Subdeployment, Oracle Role Manager JMSSubdeployment is created.
 - h. Notification Topic, Oracle Role Manager NotificationTopic is created.
 - i. Queues, Oracle Role Manager FinisherQueue, Oracle Role Manager LoaderQueue, and Oracle Role Manager IncomingEventQueue are created.
18. Set up the Commons Logging by performing the steps described in "[Setting Up Commons Logging](#)" on page A-5

Note: You must restart both WebLogic Administration server and Oracle Role Manager server for the logging to take effect.

19. Start the server and log in to the WebLogic Admin Console.
20. Set the JTA transaction timeout parameter by performing the following steps:
 - a. In the domain tree, select **Services, JTA**.

- b. In the **Timeout Seconds** field, type 1200.
- c. In the **Abandon Timeout Seconds** field, ensure that the value is 86400.
- d. Click **Save**.

Note: The value of Abandon Timeout Seconds must always be greater than Timeout Seconds and Stuck Thread Max Time.

- 21. Set the Stuck Thread Max Time parameter by performing the following steps:
 - a. In the domain tree, select **Environment, Servers, ORMServer**.
 - b. Click the **Tuning** tab.
 - c. In the **Stuck Thread Max Time** field, type 3000.
 - d. Click **Save**.

Note: The value of Stuck Thread Max Time must be at least twice that of the value of Timeout Seconds.

- 22. Configure the JMS Connection Factory by performing the following steps:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMS Module**.
 - c. In the **Name** field, select **ORM ConnectionFactory**.
 - d. Select **Default Targeting Enabled**.
 - e. Click **Save**.
 - f. Click the **Transactions** tab, ensure that the **XA Connection Factory Enabled** field is selected and then click **Save**.
 - g. In the domain tree, select **Services, Messaging, JMS Modules**.
 - h. Click **ORM JMS Module**.
 - i. In the **Name** field, select **Finalization ORM ConnectionFactory**.
 - j. Select **Default Targeting Enabled**.
 - k. Click **Save**.
 - l. Click the **Transactions** tab, ensure that the **XA Connection Factory Enabled** field is selected and then click **Save**.

- 23. In the domain tree, select **Environment, Servers, ORM Server** and navigate to the **Control** tab and click **Start** to start the managed server.

Note: You must start node manager before starting the managed server.

- 24. Click **Deployment** to start the Role Manager applications and perform the steps described in the "[Deploying Role Manager](#)" on page A-11.

4.2.2 Configuring Oracle WebLogic Server in a Clustered Mode

This section explains how to deploy Oracle Role Manager in a clustered Oracle WebLogic Server environment.

This section discusses the following topics:

- [About Oracle WebLogic Server Clusters](#)
- [Configuring WebLogic 10.3 Clusters](#)
- [Configuring Apache Failover Proxy](#)

4.2.2.1 About Oracle WebLogic Server Clusters

A clustered installation requires multiple host computers. The instructions in this chapter involve deployment and running of Oracle Role Manager on three host computers. These instructions assume that you have three computers, of which one is used to host the Web server and the other two are used for Oracle Role Manager cluster.

[Table 4–1](#) describes the entities needed for a cluster, the computers that the entities run on, and the software required for the entities. Host computers and entities are labeled.

Table 4–1 WebLogic-Based Oracle Role Manager Cluster Host Computers

Host Computers	Entities	Software	Description
Admin Server, Finalization Server and Managed Server1	WebLogic Admin Server, WebLogic Finalization Server, and WebLogic Node Manager	WebLogic Server	Administrative server for the WebLogic domain, Finalization Server and WebLogic Managed Servers
	ORM_SERVER1	Oracle Role Manager	Part of ORM_CLUSTER
	ORM_CLUSTER	Oracle Role Manager	Name of the WebLogic cluster that hosts Oracle Role Manager (logical entity).
Managed Server2	ORM_SERVER2	Oracle Role Manager	WebLogic Managed Server 2
	WebLogic Node Manager		Part of ORM_CLUSTER
	ORM_CLUSTER		Name of the WebLogic cluster that hosts Oracle Role Manager (logical entity).
Web Server	Apache Web Server	Apache HTTP Server 2.2 with WebLogic 10.3 Apache plugin	Apache Failover Proxy

Caution: Deploying an application in a clustered installation is a complex procedure. This document assumes that you have expertise in installing and running applications on an Oracle WebLogic Server cluster. This chapter provides Oracle Role Manager-specific information only. It does not cover the procedure to set up an Oracle WebLogic Server cluster. For more information about clustering, refer to Oracle WebLogic Server documentation.

4.2.2.2 Configuring WebLogic 10.3 Clusters

The instructions mentioned in this section are for installing Role Manager in a WebLogic cluster of two machines with two Role Manager servers, one Admin Server and one finalization server. Therefore there are four servers, first machine hosts

Admin, Finalization, and Managed Server1 and the second machine hosts Managed Server2. In addition, the data store for the queues are going to be database-based and not file-based.

To configure WebLogic 10.3 in a cluster mode:

1. On the primary node, complete the single instance of WebLogic server 10.3 configuration, install and deploy Role Manager, load sample data, and ensure that the server is running. Refer to "[Configuring Oracle WebLogic Server in a Nonclustered Mode](#)" on page 4-1 for instructions on configuring the WebLogic server 10.3. The following are the configuration details for the primary node:

Host: PRIMARY_NODE

Machine: ORM_Machine

BEA_Home: BEA_HOME

WLS_HOME: WLS_HOME

DOMAIN_HOME: DOMAIN_HOME

ADMIN_PORT: ADMIN_PORT

ORM server: ORMServer

ORM server Port: ORMServer_Port (9001)

Node_manager Port: NODE_MANAGER_PORT (5556, ssl)

To control your Managed Servers remotely from the Administrative Server, you must set up and configure Node Manager on each of the remote systems hosting Managed Servers by following the instructions on the BEA e-docs page:

http://e-docs.bea.com/wls/docs103/nodemgr/nodemgr_config.html

On each remote computer, on which BEA WebLogic Server is installed and Managed Servers are configured, edit the nodemanager.hosts file and specify the IP address/DNS Name (set ReverseDnsEnabled=true in the nodemanager.properties file to use DNS name) of the Administrative Server host.

Note: After installing BEA WebLogic Server, you must start (or restart) the Node Manager to generate the initial nodemanager.hosts file.

The default location of the nodemanager.hosts and nodemanager.properties files is:

For Microsoft Windows:

BEA_HOME\wlserver_10.3\common\nodemanager

For UNIX:

BEA_HOME/wlserver_10.3/common/nodemanager

2. Install WebLogic 10.3 on a secondary node.
3. Start the node manager on both the nodes.
4. Log in to the administrative server on the primary node.
5. Shutdown ORMServer on the primary node as follows:
 - a. In the domain tree, select **Environment, Servers**.

- b. Click the **Control** tab.
 - c. Select **ORM Server** and then click **Shutdown**.
6. Create a Machine, for example, `ORM_Machine1` for the secondary node as follows:
 - a. In the domain tree, select **Environment, Machines**.
 - b. Click **New**.
 - c. In the **Name** field, type `ORM_Machine1`.
 - d. Click **OK**.
7. Configure the machine to access Node Manager on secondary machine as follows
 - a. In the domain tree, select **Environment, Machines**.
 - b. Click on the machine that you created, for example, `ORM_Machine1`.
 - c. Click the **Node Manager** tab.
 - d. In the **Listen Address** field, type the IP address of the secondary node and click **Save**.
8. Create a server, for example, `ORMServer1` which uses the port, for example, `ORMServer_Port1 (7071)` as follows:
 - a. In the domain tree, select **Environment, Servers**.
 - b. Click **New**.
 - c. In the **Server Name** field, type `ORM_Server1`.
 - d. In the **Server Listen Port** field, type `7071`.
 - e. Click **Finish**.
9. Ensure that `ORMServer1` is assigned to `ORM_Machine1` as follows:
 - a. In the domain tree, select **Environment, Machines, ORM_Machine1, Node Manager**.
 - b. Check whether the IP address is same as the secondary node.
 - c. Click the **Servers** tab and select **Add**.
 - d. Select **Select an existing server, and associate it with this machine** and from the **Select a server** list, select `ORMServer1`.
 - e. Click **Next** and then click **Finish**.

The following are the configuration details of the secondary node:

Host: `SECONDARY_NODE`

Machine: `ORM_Machine1`

BEA_Home: `BEA_HOME1`

WLS_HOME: `WLS_HOME1`

DOMAIN_HOME: No domain yet

ADMIN_PORT: No admin server on secondary node

ORM server: `ORMServer1`

ORM server Port: `ORMServer_Port1 (7071)`

Node_manager Port: `NODE_MANAGER_PORT1 (5556, ssl)`

10. Create cluster as follows:
 - a. In the domain tree, select **Environment, Clusters**.
 - b. Click **New**.
 - c. In the **Name** field, type `ORMCluster`.
 - d. Click **OK**.
 - e. In the domain tree, select **Environment, Clusters**.
 - f. Click **ORMCluster**.
 - g. Click **Configuration** tab and then click **Servers** tab.
 - h. Click **Add** to add a server to cluster.
 - i. Select the server, `ORM_Server` and click **Finish**.
 - j. Repeat the steps e to i and select the second server, `ORM_Server1`.
11. Configure the JDBC data sources as follows:
 - a. In the domain tree, select **Environment, Services**.
 - b. In the Summary of Services section, select **JDBC, Data Sources**.
 - c. Click **ORM Data Source**.
 - d. Click the **Targets** tab.
 - e. Select **ORMCluster, All servers in the cluster**.
 - f. Click **Save**.
 - g. Repeat the steps a to f for **ORM XA Data Source**, except that in the Step c, click **ORM XA Data Source**.
12. Create a JDBC Store as follows:
 - a. In the domain tree, select **Services**.
 - b. Click **Persistent Stores**.
 - c. Click **New** and select **Create JDBC Store** from the list.
 - d. In the **Name** field, type `JDBCStore`.
 - e. In the **Target** field, select **ORMServer**.
 - f. In the **DataSource** field, select **ORM Data Source**.
 - g. In the **Prefix Name** field, type `jdbctestore`.
 - h. Click **OK**.
13. Create another JDBC Store as follows:
 - a. In the domain tree, select **Services**.
 - b. Click **Persistent Stores**.
 - c. Click **New** and select **Create JDBCStore** from the list.
 - d. In the **Name** field, type `JDBCStore1`.
 - e. In the **Target** field, select **ORMServer1**.
 - f. In the **DataSource** field, select **ORM Data Source**.
 - g. In the **Prefix Name** field, type `jdbctestore1`.

- a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Select **ORM NotificationTopic, ORM FinisherQueue, ORM LoaderQueue, ORM IncomingEventQueue**.
 - d. Click **Delete**.
20. Recreate the Oracle Role Manager NotificationTopic as follows:
- a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Click **New**.
 - d. Select **Distributed Queue**.
 - e. In the **JNDI Name** field, type `orm/topic/NotificationTopic`.
 - f. Click **Save**.
21. Recreate the Oracle Role Manager LoaderQueue as follows:
- a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Click **New**.
 - d. Select **Distributed Queue**.
 - e. In the **JNDI Name** field, type `orm/queue/LoaderQueue`.
 - f. Click **Save**.
22. Recreate the Oracle Role Manager IncomingEventQueue as follows:
- a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Click **New**.
 - d. Select **Distributed Queue**.
 - e. In the **JNDI Name** field, type `orm/queue/IncomingEventQueue`.
 - f. Click **Save**.
23. Create a server, `ORMFinalizationServer` as follows:

Note: The new server can be in a different domain, or in the same domain, but not in the cluster.

- a. In the domain tree, select **Environment, Servers**.
 - b. Click **New**.
 - c. In the **Server Name** field, type `ORMFinalizationServer`.
 - d. In the **Server Listen Port** field, type `7074`.
24. Configure a machine for the Oracle Role Manager FinalizationServer as follows:
- a. In the domain tree, select **Environment, Servers**.
 - b. Click **ORMFinalizationServer**.

- c. Click **Machine** and select the host computer on which the server is run.
25. Create a JMS Server as follows:
 - a. In the domain tree, select **Services, Messaging**.
 - b. Click **JMS Servers**.
 - c. Click **New**.
 - d. In the **Name** field, type `FinalizationJMSServer`.
 - e. Click **Next**.
 - f. In the **Target** field, type `ORMFinalizationServer`.
 - g. Click **Finish**.
26. Create a JMS module as follows:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **New**.
 - c. In the **Name** field, type `FinalizationJMSModule`.
 - d. Click **Next**.
 - e. In the **Target** field, type `ORMFinalizationServer`.
 - f. Click **Finish**.
27. Create a Subdeployment in the JMS module as follows:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **FinalizationJMSModule**.
 - c. Click the **Subdeployments** tab.
 - d. Click **New**.
 - e. In the **Subdeployment Name** field, type `ORM Subdeployment`.
 - f. Click **Next** and select **FinalizationJMSServer** as the target server.
 - g. Click **Finish**.
28. Create a connection factory as follows:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **FinalizationJMSModule**.
 - c. Click **New**.
 - d. Select **Connection Factory** and click **Next**.
 - e. In the **Name** field, type `Finalization ORM ConnectionFactory` and click **Next**.
 - f. In the **JNDI Name** field, type `orm/remote/jms/FinalizationConFac`.
 - g. Click **Next** and then click **Finish**.
 - h. Click **Finalization ORM ConnectionFactory**.
 - i. Click the **Transactions** tab.
 - j. Select **XA Connection Factory Enabled**.
 - k. Click **Save**.

29. Create a queue as follows:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **FinalizationJMSModule**.
 - c. Click **New**.
 - d. Select **Queue** and click **Next**.
 - e. In the **Name** field, type `ORM FinalizationQueue`.
 - f. In the **JNDI Name** field, type `orm/remote/queue/BtFinisherQueue`.
 - g. Click **Next**.
 - h. In the **Subdeployments** field, select `ORM JMSSubdeployment`.
 - i. Click **Finish**.
30. Change the configuration of Oracle Role Manager Data Source to target `ORMFinalizationServer` as follows:
 - a. In the domain tree, select **Environment, Services, JDBC, Data Sources**.
 - b. Click **ORM Data Source**.
 - c. Click the **Targets** tab.
 - d. Select **ORMFinalizationServer**, and ensure that **ORMCluster** is selected.
 - e. Click **Save**.
31. Create a JDBC Store as follows:
 - a. In the domain tree, select **Services, JDBC, Persistent Stores**.
 - b. Click **Persistent Stores**.
 - c. Click **New** and select **Create JDBCStore** from the list.
 - d. In the **Name** field, type `ORMJDBCStoreF`.
 - e. In the **Target** field, select **ORMFinalizationServer**.
 - f. In the **DataSource** field, select **ORM Data Source**.
 - g. In the **Prefix Name** field, type `ORMF`.
 - h. Click **OK**.
32. Create a foreign server as follows:
 - a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Click **New**.
 - d. Select **Foreign Server** and click **Next**.
 - e. In the **Name** field, type `FinalizationServer` and click **Next**.
 - f. Click **Finish**.
 - g. Click **FinalizationServer**.
 - h. In the **JNDI Initial Context Factory** field, type `weblogic.jndi.WLInitialContextFactory`.
 - i. In the **JNDI Connection URL** field, type `t3://machine_name:7074`.

Note: The `machine_name` is the name of the machine where `ORMFinalizationServer` is deployed.

- j. Select **Default Targeting Enabled**.
 - k. Click **Save**.
 - l. Click the **Destinations** tab and click **New**.
 - m. In the **Name** field, type `ORM FinalizationQueue`.
 - n. In the **Local JNDI Name** field, type `orm/queue/BtFinisherQueue`.
 - o. In the **Remote JNDI Name** field, type `orm/remote/queue/BtFinisherQueue`.
 - p. Click **OK**.
 - q. Click the **Connection Fatories** tab and click **New**.
 - r. In the **Name** field, type `ORM Finalization ConnectionFactory`.
 - s. In the **Local JNDI Name** field, type `orm/jms/FinalizationConFac`.
 - t. In the **Remote JNDI Name** field, type `orm/remote/jms/FinalizationConFac`.
 - u. Click **OK**.
33. Configure the connection factory as follows:
- a. In the domain tree, select **Services, Messaging, JMS Modules**.
 - b. Click **ORM JMSModule**.
 - c. Click **ORM ConnectionFactory**.
 - d. Deselect **Default Targeting Enabled**.
 - e. Click **Save**.
 - f. Click **Subdeployment** tab.
 - g. In the **Subdeployment** field, select `cf-sub` and click **Save**.
34. Change the deployed applications (`ORMServerApp` and `webui`) to `All servers in the cluster` as target.
35. Pack/unpack the domain to secondary node as follows:

Note: Ensure that all server node managers are running while performing the following steps.

- a. On primary node, run the following command:

```
>cd <WLS_HOME>/common/bin
>pack.cmd -domain=$DOMAIN_HOME -template=/tmp/template_x.jar
-template_name="template_x" -managed=true
```

- b. Copy `template_x.jar` to secondary node.

On secondary node, run the following command:

```
>cd $WLS_HOME/common/bin
>unpack.cmd -template=??/template_x_orm.jar -domain=$DOMAIN_HOME
```

36. Configure SSL as follows:

- a.** In the domain tree, select **Environment, Servers**.
- b.** Click AdminServer(admin).
- c.** Click the **SSL** tab.
- d.** Click **Advanced**.
- e.** In the **Hostname Verification** field, select **None**.
- f.** Repeat Steps a to e for ORMFinalization Server, ORMServer, and ORMServer1.

Note: You must perform this step only when there is a certificate failure error.

Note:

- Start ORMFinalizationServer before starting the Managed Server.
- If you are starting ORMServer1 for the first time, you must start it manually once using the following command from:

```
startManagedWebLogic.sh ORMServer1
http://primary_node:adminport
```

4.2.2.3 Configuring Apache Failover Proxy

To configure Apache failover proxy:

- 1.** Install Apache HTTP server 2.2.
- 2.** Download the weblogic apache plugin from:
<http://www.oracle.com/technology/products/weblogic/index.html>
- 3.** Unzip and copy:
win/mod_wl_22.so to apache_home/modules directory
- 4.** Add the following to httpd.conf file:

```
LoadModule weblogic_module modules/mod_wl_22.so

<IfModule mod_weblogic.c>
    WebLogicCluster node1_ip:port,node2_ip:port
</IfModule>

<Location /webui>
    SetHandler weblogic-handler
</Location>

<Location /ormconsole>
    SetHandler weblogic-handler
</Location>
```
- 5.** Restart Apache and all weblogic servers.

You must be able to access webui and console at:

`http://myApacheServer/webui`
`http://myApacheServer/ormconsole`

4.3 Configuring JBoss

This procedure assumes that JBoss is installed on the application server host for Role Manager.

You must configure JBoss server in SSL mode to operate in a secure environment. For information about configuring SSL for JBoss server, refer to the following URL:

http://docs.jboss.org/jbossas/guides/webguide/r2/en/html_single/#ch9.https.sec

To configure JBoss for Role Manager

1. Copy the `orm-ds.xml` and `orm-service.xml` files from:

```
<ORM_install>/samples/jboss/4.2.3
```

to the JBoss server where you want to deploy Role Manager. For example:

```
<JBOSS_HOME>/server/default/deploy
```

2. Include the following connection strings in `orm-ds.xml` file:

- a. If you are using Oracle RAC database:

```
<connection-url>jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = host1-vip) (PORT = 1521)) (ADDRESS = (PROTOCOL = TCP) (HOST = host2-vip) (PORT = 1521)) (LOAD_BALANCE = yes) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = db-service)))</connection-url>
```

- b. If you are not using Oracle RAC database:

```
<connection-url>jdbc:oracle:thin:@//SERVER_NAME:1521/SERVICE_NAME</connection-url>
```

3. Set the session ID to false in the following path:

```
JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml file  

setting emptySessionPath="false" for the HTTP/1.1 Connector
```

4. Set the JTA transaction timeout parameter by performing the following steps:

- a. Open the `jboss-service.xml` file from the following path:

```
%JBOSS_HOME%/server/default/conf/jboss-service.xml file
```

- b. Locate the configuration for mbean with the name, "jboss:service=TransactionManager".

- c. Change the `TransactionTimeout` attribute value to 1200:

```
<attribute name="TransactionTimeout">1200</attribute>
```

Note: For more information about the JBoss Application Server, refer to the following link:

<http://www.jboss.org/docs/>

5. Encrypt the password of the Role Manager application user defined in "[Creating the Role Manager Users](#)" on page 3-3 (refer to [Section 4.3.1](#) for instructions).
6. Edit the orm-ds.xml file as follows:

- a. Change the two occurrences of `connection-url` to match your database environment:

```
<connection-url>jdbc:oracle:thin:@//SERVER_NAME:PORT/SERVICE_NAME</connection-url>
```

- b. Change the two occurrences of `user-name` and `password` to match the credentials of the Role Manager application user with the newly encrypted password:

```
<user-name>USER_NAME</user-name>  
<password>PASSWORD</password>
```

Note: This step is optional. Perform this step for development or non-production environments, where password encryption is not needed.

7. Copy the server.ear file from `<ORM_install>/lib` to the JBoss directory used above.
8. Copy the webui.war file from `<ORM_install>/webui/jboss/4.2.3` to the JBoss directory used above.
9. If JBoss is not already running, start the JBoss server using the following command:

For UNIX-based systems:

```
<JBoss Install Location>/bin/run.sh
```

For Windows systems:

```
<JBoss Install Location>\bin\run.bat
```

10. To test the server installation, ensure that you can get to the Role Manager administrative console from a Web browser. For example:

```
http://localhost:8080/ormconsole
```

11. To test the Role Manager Web application installation:

- a. In a Web browser, navigate to the Role Manager Web UI. For example:

```
http://localhost:8080/webui
```

- b. Log in as the Role Manager Administrator created in "[Installing Role Manager](#)" on page 3-3

You should be able to see the Home page of the Role Manager Web application.

Note: Data must be loaded into the system to expose all the functionality of the application. Refer to "[Loading Standard and Sample Data](#)" on page 5-1 for instructions.

4.3.1 Encrypting the Role Manager Database Password

This section describes how to encrypt the Role Manager database password in JBoss application server deployments. Specifically, you must perform the following steps to manually encrypt a password, and then modify the `orm-ds.xml` and `login-config.xml` files so that they can access the encrypted form of the password instead of the clear text version.

To encrypt the Role Manager database password:

1. Open a console window and navigate to the `JBOSS_HOME` directory.
2. Stop the JBoss server.
3. Run one of the following commands to encrypt the Role Manager database password. In this command, replace `password` with the actual password that you want to encrypt.

For UNIX-based systems:

```
java -cp
"$JBOSS_HOME/lib/jboss-jmx.jar:$JBOSS_HOME/lib/jboss-common.jar:$JBOSS_HOME/ser
ver/default/lib/jboss-jca.jar:$JBOSS_HOME/server/default/lib/jbosssx.jar"
org.jboss.resource.security.SecureIdentityLoginModule password
```

For Windows systems:

```
java -cp
"%JBOSS_HOME%/lib/jboss-jmx.jar;%JBOSS_HOME%/lib/jboss-common.jar;%JBOSS_HOME%
/server/default/lib/jboss-jca.jar;%JBOSS_HOME%/server/default/lib/jbosssx.jar"
org.jboss.resource.security.SecureIdentityLoginModule password
```

This command returns an encoded form of the password you specify. For example, the password `Welcome1` is encoded as `3146f9cc50afd6a6df8592078de921bc`.

4. Highlight and copy the encoded password to paste later in the JBoss application policy element definitions.
5. Open the `JBOSS_HOME/server/default/deploy/orm-ds.xml` file in a text editor.
6. Delete the `<user-name>` and `<password>` elements from the `<no-tx-datasource>` element.
7. Add the following `<security-domain>` element to the end of the `<no-tx-datasource>` element:


```
<security-domain>EncryptDBPassword</security-domain>
```
8. Delete the `<user-name>` and `<password>` elements from the `<local-tx-datasource>` element.
9. Add the following `<security-domain>` element to the end of the `<local-tx-datasource>` element:


```
<security-domain>EncryptXADBPassword</security-domain>
```
10. Save and close the `orm-ds.xml` file.
11. Open the `JBOSS_HOME/server/default/conf/login-config.xml` file in a text editor.
12. Add the following to `<application-policy>` element at the end of the `<policy>` element while replacing `datasource_username` with the data source

user name and *encoded_password* with the encoded password you copied in step 3:

```
<application-policy name = "EncryptXADBPassword">
  <authentication>
    <login-module code = "org.jboss.resource.security.SecureIdentityLoginModule"
flag = "required">
      <module-option name = "username">datasource_username</module-option>
      <module-option name = "password">encoded_password</module-option>
      <module-option name = "managedConnectionFactoryName">
        jboss.jca:service=LocalTxCM,name=ORMServerXADS</module-option>
    </login-module>
  </authentication>
</application-policy>

<application-policy name = "EncryptDBPassword">
  <authentication>
    <login-module code = "org.jboss.resource.security.SecureIdentityLoginModule"
flag = "required">
      <module-option name = "username">datasource_username</module-option>
      <module-option name = "password">encoded_password</module-option>
      <module-option name = "managedConnectionFactoryName">
        jboss.jca:service=NoTxCM,name=ORMServerDS</module-option>
    </login-module>
  </authentication>
</application-policy>
```

13. Save and close the login-config.xml file.

4.3.2 Configuring Data Upload Size Limit

You can upload a DAR file to load data of maximum size one byte into the system. If you try to load data larger than this maximum upload size, you get an error message. You can configure the maximum data upload size limit to a higher or lower value than the default settings.

To configure the data upload size limit:

1. Edit the config file:

For UNIX-based systems:

```
JBOSS_HOME/bin/run.sh
```

For Windows systems:

```
JBOSS_HOME/bin/run.bat
```

2. Add the following argument to JAVA_OPTS:

```
-Doracle.iam.rm.loader.max_upload_size=<new_value>
```

4.4 Configuring IBM WebSphere

This procedure assumes that a WebSphere application server profile has been created for Role Manager with a host alias set for port access to Role Manager.

Note:

- During profile creation, you must select the option to enable administrative security.
 - When configuring WebSphere, it is recommended that you save your settings after every task.
-
-

You must configure IBM WebSphere server in SSL mode to operate in a secure environment. For information about configuring SSL for WebSphere server, refer to the following URL:

<http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/welc6topsecureihs.html>

This section includes the following subsections:

- [Creating a Non-Administrative Server for Deploying Oracle Role Manager](#)
- [Configuring WebSphere to Use a Non-Default HTTP Port](#)
- [Configuring JDBC Providers](#)
- [Reconfiguring JDBC Providers](#)
- [Creating the Role Manager Database Credentials](#)
- [Configuring the Non-XA Data Source](#)
- [Configuring the Transaction \(XA\) Data Source](#)
- [Configuring the JMS messaging buses](#)
- [Configuring Bus Destinations](#)
- [Configuring JMS Queue Connection Factories](#)
- [Configuring the JMS Topic Connection Factory](#)
- [Configuring JMS Queues](#)
- [Configuring the JMS Notification Topic](#)
- [Configuring JMS Activation Specifications](#)
- [Securing the WebSphere Installation/Console](#)
- [Creating a Custom User](#)
- [Creating Alias for Custom User](#)
- [Configuring Connection Factory Authentication](#)
- [Configuring Activation Specification Authentication](#)
- [Securing the Message Bus](#)
- [Configuring Data Upload Size Limit](#)
- [Increasing the Transaction Timeout](#)
- [Deploying Role Manager Server](#)
- [Deploying the Role Manager Web Application](#)

4.4.1 Creating a Non-Administrative Server for Deploying Oracle Role Manager

Oracle recommends you to deploy the Oracle Role Manager system on a non-administrative server.

To create a non-administrative server:

1. Run the following command:

```
[WebSphere Install Dir]/AppServer/profiles/[Profile name]/bin/wsadmin.bat
```

Note: You must ensure that the WebSphere server is running before performing this step.

2. On the wsadmin prompt (wsadmin>), enter the following commands:

```
$AdminTask createApplicationServer <Websphere Node Name> { -name orm  
-templateName default }  
$AdminConfig save  
quit
```

Note: The node name specified in the first command must be same as the node name of the administrative server that gets created by default, for example `server1`. You can find out the node name on the admin console by going to Servers, Application Servers.

4.4.2 Configuring WebSphere to Use a Non-Default HTTP Port

If you are deploying the system on a non-administrative server, then perform the following steps:

To configure the WebSphere application server to use a non-default port:

1. If not already on the WebSphere administrative console, in a Web browser, type the URL, for example:

```
http://<appserverhost>:9060/ibm/console
```
2. Select **Environment**, **Virtual Host**, **default_host**, **Host Aliases** and then click **New**.
3. In the **Host Name** field, type `*`.
4. In the **Port** field, enter the HTTP port number of the non-admin server on which Oracle Role Manager is deployed, for example `9081`.
5. Click **OK**.

4.4.3 Configuring JDBC Providers

To configure the transaction (XA) and non-transaction JDBC providers:

1. If not already on the WebSphere administrative console, in a Web browser, type the URL, for example:

```
http://<appserverhost>:9060/ibm/console
```

2. In the administrative console, go to Resources, JDBC, JDBC Providers.

3. Select the cell scope from the **Scope** list, and then click **New** to create the XA JDBC provider.
4. Select **Oracle** as the database type.
5. Select **Oracle JDBC Driver** as the provider type.
6. Select **XA datasource** as the Implementation type, and then click **Next**.
7. In the **Directory location** field, type the full path to the JDBC drivers, for example, <ORM_Install>/lib, and then click **Next**.

Note: You must use "/" to specify the path.

8. Click **Finish**.
9. Click **New** to create the non-XA JDBC provider.
10. Select **Oracle** as the database type.
11. Select **Oracle JDBC Driver** as the provider type
12. Select **Connection pool data source** as the Implementation type, and then click **Next**.
13. Ensure that the value in the **Directory location** field is correct, and then click **Next**.
14. Click **Finish**.

4.4.4 Reconfiguring JDBC Providers

This section is applicable only when you are using Oracle 11g JDBC driver (ojdbc5.jar) to connect to oracle 11g database.

Oracle recommends you to use ojdbc5.jar when configuring Oracle Role Manager with Oracle11g database. WebSphere Application Server by default creates Oracle JDBC providers using the Oracle 10g JDBC driver (ojdbc14.jar). In the administrative console, the wizard for creating new data sources does not allow you to change the name of the jar file. For example, you cannot change the entry from ojdbc14.jar to ojdbc5.jar. For more information about JDBC providers, refer to the following link:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rdat_minreqoracle.html

After you create the JDBC provider using the wizard, modify it to change the class path entry to reflect the location of ojdbc5.jar as follows:

To reconfigure the JDBC providers:

This procedure assumes that you have already performed the steps mentioned in "[Configuring JDBC Providers](#)" on page 4-20.

1. If not already on the WebSphere administrative console, in a Web browser, type the URL, for example: http://<appserverhost>:9060/ibm/console.
2. In the administrative console, go to Resources, JDBC, JDBC Providers.
3. Select the cell scope from the **Scope** list, and then click on JDBC provider, **Oracle JDBC Driver**.
4. In the Class path field, type the full path of the JDBC drivers ojdbc5.jar, for example, <ORM_Install>/lib/ojdbc5.jar.

5. Click **Apply**.
6. Click **Save**.

Note: You must use "/" to specify the path and ensure that ojdbc5.jar file is copied from Oracle DB install to <ORM_Install>/lib.

7. Repeat the steps from 2 to 6 for the JDBC provider, Oracle JDBC Driver (XA).

Note: You must execute these steps before creating any data sources as mentioned in "[Configuring the Non-XA Data Source](#)" on page 4-22 and "[Configuring the Transaction \(XA\) Data Source](#)" on page 4-23. If the data sources are already created, then you must recreate after deleting them.

4.4.5 Creating the Role Manager Database Credentials

To create the Role Manager Database Alias:

1. Go to Security, Secure administration, applications, and infrastructure.
2. In the Authentication area, select **Java Authentication and Authorization Service** and then click the **J2C authentication data** link.
3. Click **New**.
4. Type a name for the alias, for example, ORM Database to identify the Role Manager database.
5. Type the user ID and password for the Role Manager application user as specified in "[Creating the Role Manager Users](#)" on page 3-3.
6. Click **OK**.

4.4.6 Configuring the Non-XA Data Source

To configure the non-XA data source and credentials:

1. Go to Resources, JDBC, Data sources.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. In the **Data source name** field, type a name for the non-XA data source, for example, ORM Non-XA Data source.
4. In the **JNDI name** field, type orm/jdbc/ORMServerDS, and then click **Next**.
5. Choose an existing JDBC provider and select the non-XA JDBC provider you created in the Step 9 of "[Configuring JDBC Providers](#)" on page 4-20, for example, **Oracle JDBC Driver**, and then click **Next**.
6. In the **URL** field, type the JDBC connection URL:

```
jdbc:oracle:thin:@<server>[:<port>]:<database_name>
```

For example:

```
jdbc:oracle:thin:@localhost:1521:orcl
```

7. Select **Oracle10g data store helper** from the list, and then click **Next**.

Note: You must use Oracle11g data store helper for Oracle 11g database.

8. Click **Finish**.
The non-XA data source for Role Manager should appear in the list.
9. Click the name of the new non-XA data source to display details.
10. In the Container-managed authentication alias list, select the database alias created in the Step 4 of "[Creating the Role Manager Database Credentials](#)" on page 4-22 and then click **Apply**.
The reference to this option being deprecated can be ignored.
11. On the same page, in the Additional Properties section, click Connection Pool Properties and set the Maximum connections to 30.
12. Click **OK**.

4.4.7 Configuring the Transaction (XA) Data Source

To configure the XA data source:

1. Go to Resources, JDBC, Data sources.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. In the **Data source name** field, type a name for the XA data source, for example, `ORM XA Data source`.
4. In the **JNDI name** field, type `orm/jdbc/ORMServerXADS`, and then click **Next**.
5. Choose an existing JDBC provider and select the XA JDBC provider that you created in "[Configuring JDBC Providers](#)" on page 4-20, for example, **Oracle JDBC Driver (XA)**, and then click **Next**.
6. In the **URL** field, type the JDBC connection URL:
`jdbc:oracle:thin:@<server>[:<port>]:<database_name>`
For example:
`jdbc:oracle:thin:@localhost:1521:orcl`
7. Select **Oracle10g data store helper** from the list, and then click **Next**.

Note: You must use Oracle11g data store helper for Oracle 11g database.

8. Click **Finish**.
Both the new XA data source and non-XA data source for Role Manager must appear in the list.
9. Click the name of the XA data source to display details.
10. In the Container-managed authentication alias list, select the database alias created in "[Creating the Role Manager Database Credentials](#)" on page 4-22, and then click **Apply**.

The reference to this option being deprecated can be ignored.

11. On the same page, in the Additional Properties section, click **Connection Pool Properties** and set the Maximum connections to 30.
12. Click **OK**.

4.4.8 Configuring the JMS messaging buses

To configure the JMS messaging buses:

1. Select **Service integration, Buses**, and then click **New**.
2. Type a name for the Role Manager bus, such as `ORM Bus`, and deselect the **Bus security** check box, and then click **Next**.
3. Click **Finish**.
4. Click **New** to create the finalization bus.
5. Type a name for the finalization bus, such as `ORM Finalization Bus`, and deselect the **Bus security** check box, and then click **Next**.

Note: ■ If you do not set the name to "ORM Finalization Bus", you must provide the "oracle.iam.rm.finalization.WebSphereFinalizationBusName" system property with the name that you use.

- If you want to use a different name for the finalization bus, you must follow the Step 6 to set the `WebSphereFinalizationBusName` property. Otherwise, skip the next step.
-
-

6. If you use a name other than `ORM Finalization Bus`:
 - a. Select **Servers, Application Servers**.
 - b. Click the server on which Role Manager is installed.
 - c. In the Server Infrastructure section, click **Java and Process Management, Process Definition**.
 - d. Click **Java Virtual Machine**.
 - e. Click **Custom Properties**.
 - f. Click **New**.
 - g. In the **Name** field, type the following text:
`oracle.iam.rm.finalization.WebSphereFinalizationBusName`
 - h. In the **Value** field, type the name you set for the finalization bus.
 - i. Click **OK**.
 - j. Click **Finish**.
7. Add the server to each of the newly created buses as follows:
 - a. Click the bus link, and then click **Bus members**.
 - b. Click **Add**.
 - c. Select the server to use for Role Manager, and then click **Next**.

- d. In the **Select the type of message store** list, select **File Store**, click **Next**, and then click **Next** again.
- e. Click **Finish**.

4.4.9 Configuring Bus Destinations

To configure the Role Manager Bus and Finalization Bus destinations:

1. If not already on the Buses page, go to Service integration, Buses.
2. Click the **ORM Bus** link, and then click **Destinations**.
3. Click **New**.
4. Select **Queue** as the destination type, and then click **Next**.
5. Type `Loader Queue` as the identifier, and then click **Next**.
6. Specify the bus member to own the queue, and then click **Next**.
7. Click **Finish**.
8. Repeat these steps, but this time, type `Incoming Event Queue` as the identifier.
9. Click **New**, select **Topic space**, and then click **Next**.
10. Type `Notification Topic` as the identifier, and then click **Next**.
11. Click **Finish**.
12. Click **ORM Finalization Bus** (or alternate finalization bus, if created in [Section 4.4.8](#)), and then click **Destinations**.
13. Click **New**.
14. Choose **Queue** as the destination type, and then click **Next**.
15. Type `Finisher Queue` as the identifier, and then click **Next**.
16. Specify the bus member to own the queue, and then click **Next**.
17. Click **Finish**.

4.4.10 Configuring JMS Queue Connection Factories

To configure JMS queue connection factories:

1. Go to Resources, JMS, Queue connection factories.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Choose **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type a name for the Role Manager connection factory, such as `ORM QCF`.
5. In the **JNDI name** field, type `orm/jms/QueueConFac`.
6. In the **Bus name** list, select **ORM Bus**, and then click **OK**.
7. Click **New**.
8. Select **Default messaging provider**, and then click **OK**.
9. In the **Name** field, type a name for the Role Manager connection factory for finalization, such as `ORM Finalization QCF`.

10. In the **JNDI name** field, type `orm/jms/FinalizationQueueConFac`.
11. In the **Bus name** list, select **ORM Finalization Bus** (or alternate finalization bus, if created in [Section 4.4.8](#)).
12. Click **OK**.

4.4.11 Configuring the JMS Topic Connection Factory

To configure the JMS topic connection factory:

1. Go to Resources, JMS, Topic connection factories.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Select **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type a name for the Role Manager topic connection factory, such as `ORM TCF`.
5. In the **JNDI name** field, type `orm/jms/TopicConFac`.
6. In the **Bus name** list, select **ORM Bus**.
7. Click **OK**.

4.4.12 Configuring JMS Queues

To configure the Loader queue:

1. Go to Resources, JMS, Queues.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Select **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Loader`.
5. In the **JNDI name** field, type `orm/jms/LoaderQueue`.
6. In the **Bus name** list, select **ORM Bus**.
7. In the **Queue name** list, select **Loader Queue**.
8. Click **OK**.

To configure the Incoming Event queue:

1. Go to Resources, JMS, Queues.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Choose **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Incoming Event Queue`.
5. In the **JNDI name** field, type `orm/jms/IncomingEventQueue`.
6. In the **Bus name** list, select **ORM Bus**.
7. In the **Queue name** list, select **Incoming Event Queue**.
8. Click **OK**.

To configure the Finalization queue:

1. Go to Resources, JMS, Queues, select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
2. Select **Default messaging provider**, and then click **OK**.
3. In the **Name** field, type `ORM Finisher Queue`.
4. In the **JNDI name** field, type `orm/jms/FinisherQueue`.
5. In the **Bus name** list, select **ORM Finalization Bus** (or alternate finalization bus, if created in "[Configuring the JMS messaging buses](#)" on page 4-24).
6. In the **Queue name** list, select **Finisher Queue**.
7. Click **OK**.

4.4.13 Configuring the JMS Notification Topic

To configure the Notification Topic:

1. Go to Resources, JMS, Topics.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Select **Default messaging provider**, and then click **OK**.
4. In the **Name** and the **Topic Name** fields, type `ORM Notification Topic`.
5. In the **JNDI name** field, type `orm/jms/NotificationTopic`.
6. In the **Bus name** list, select **ORM Bus**.
7. In the **Topic space** list, select **Notification Topic**.
8. Click **OK**.

4.4.14 Configuring JMS Activation Specifications

To configure the Loader AS:

1. Go to Resources, JMS, Activation specifications.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Select **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Loader AS`.
5. In the **JNDI name** field, type `orm/jms/LoaderAS`.
6. In the **Destination type** list, select **Queue**.
7. In the **Destination JNDI name** field, type `orm/jms/LoaderQueue`.
8. In the **Bus name** list, select **ORM Bus**.
9. Click **OK**.

To configure the Incoming Event AS:

1. Go to Resources, JMS, Activation specifications.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.

3. Select **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Incoming Event AS`.
5. In the **JNDI name** field, type `orm/jms/IncomingEventAS`.
6. In the **Destination type** list, select **Queue**.
7. In the **Destination JNDI name** field, type `orm/jms/IncomingEventQueue`.
8. In the **Bus name list**, select **ORM Bus**.
9. Click **OK**.

To configure the Finisher AS:

1. Go to Resources, JMS, Activation specifications.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Choose **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Finisher AS`.
5. In the **JNDI name** field, type `orm/jms/FinisherAS`.
6. In the **Destination type** list, select **Queue**.
7. In the **Destination JNDI name** field, type `orm/jms/FinisherQueue`.
8. In the **Bus name list**, select **ORM Finalization Bus** (or alternate finalization bus, if created in "[Configuring the JMS messaging buses](#)" on page 4-24).
9. In the **Maximum concurrent endpoints** field, set the value to 1.

Note: You must set the value of Maximum concurrent endpoints as 1 to ensure the ORM application to function properly.

10. Click **OK**.

To configure the Notification AS:

1. Go to Resources, JMS, Activation specifications.
2. Select the same cell scope used in "[Configuring JDBC Providers](#)" on page 4-20, and then click **New**.
3. Choose **Default messaging provider**, and then click **OK**.
4. In the **Name** field, type `ORM Notification AS`.
5. In the **JNDI name** field, type `orm/jms/NotificationAS`.
6. In the **Destination type** list, select **Topic**.
7. In the **Destination JNDI name** field, type `orm/jms/NotificationTopic`.
8. In the **Bus name list**, select **ORM Bus**.
9. Click **OK**.

4.4.15 Securing the WebSphere Installation/Console

To secure the WebSphere installation/console:

1. In a Web browser, type the URL to connect to the WebSphere administrative console. For example:

```
http://<appserverhost>:9060/ibm/console
```
2. Go to Security, Secure administration, applications, and infrastructure.
3. Click **Security Configuration Wizard**.
4. Select **Enable application security** and **Use Java 2 security to restrict application access to local resources** check boxes and then click **Next**.
5. In the **Select user repository**: section, select **Federated repositories** and then click **Next**.
6. Type username and password for administrative user, for example, `websphere/websphere` and then click **Next**.

Note: The username and password specified in this step must be the same as the username and password used to log in to the administrative console.

7. Click **Finish**.
8. Clear the **Warn if applications are granted custom permissions** check box.
9. Click **Apply**, and then save your changes.
10. From Servers, Application Servers, click the server on which Role Manager is to be deployed.
11. In the Server Infrastructure section, click **Java and Process Management**, and then click **Process Definition**.
12. In the Additional Properties section, click **Java Virtual Machine**.
13. In the Additional Properties section, click **Custom Properties**.
14. Click **New**.
15. In the **Name** field, type `com.ibm.websphere.java2secman.nolog`.
16. In the **Value** field, type `true`.
17. In the **Description** field, type `Stop overlogging of security warnings`.
18. Click **OK**, and then click **Save**.

4.4.16 Creating a Custom User

To create a custom user:

1. Log in to the Administrative Console.
2. Go to Users and Groups, Manage Users.
3. Click **Create** and type the following:
 - a. User ID, for example, `ormserver`.

- b. First Name, for example, `ORM`.
 - c. Last Name, for example, `Server`.
 - d. Password, for example, `ormserver`.
 4. Click **Create**, and then click **Close**.
 5. Go to Users and Groups, Administrative User Roles.
 6. Click **Add** and perform the following substeps:
 - a. In the **User** field, type the user ID created in Step 3.
 - b. In the **Role(s)** field, select **Operator**.
 - c. Click **OK**.

4.4.17 Creating Alias for Custom User

To create alias for the custom user:

1. Go to Security, Secure administration, applications, and infrastructure.
2. In the Authentication section, expand **Java Authentication and Authorization Service** and then click **J2C authentication data**.
3. Click **New** and perform the following substeps:
 - a. In the **Alias** field, type the alias name, for example, `ormserver`.
 - b. In the **User** field, type the User ID that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29.
 - c. In the **Password** field, type the password that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29.
4. Click **OK**.

4.4.18 Configuring Connection Factory Authentication

To configure authentication for the connection factories:

1. Go to Resources, Resource Adapters, J2C connection factories.
2. Click the title of the connection factory.
3. Set the Container-managed authentication alias to the custom user alias created in "[Creating Alias for Custom User](#)" on page 4-30,, and then click **OK**.
The reference to this option being deprecated can be ignored.
4. Repeat these steps for each of the new connection factories, then save your changes.

4.4.19 Configuring Activation Specification Authentication

To configure authentication for the activation specifications:

1. Go to Resources, Resource Adapters, J2C activation specification.
2. Click the title of the new activation specification.
3. Set the Authentication alias to the user alias created in "[Creating Alias for Custom User](#)" on page 4-30, and then click **OK**.

4. Repeat these steps for each of the new activation specifications, and then save your changes.

4.4.20 Securing the Message Bus

To secure the message bus:

1. Go to Security, Bus Security.
2. In the Security column, for each Oracle Role Manager bus, click **Disabled**.
3. Select the **Enable bus security** check box, and then click **Apply**.

Note: Enable bus security field is disabled if you have deselected Enable Bus Security field while configuring JMS messaging buses in the step 5 of the "[Configuring the JMS messaging buses](#)" on page 4-24.

4. For each Oracle Role Manager Bus enabled, in the Additional Properties section, click **Users and groups in the bus connector role**.
5. Click **New** and select **User Name**.
6. In the **User Name** field, type the User ID that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29, and click **OK**.

4.4.21 Configuring Data Upload Size Limit

You can upload a DAR file to load data of maximum size 10 MB into the system. If you try to load data larger than this maximum upload size, you get an error message. *Optionally*, you can configure the maximum data upload size limit to a higher or lower value than the default settings.

To configure the data upload size limit:

1. Go to Servers, Application Servers, ORM Server.
2. In the **Server Infrastructure** section, expand **Java and Process Management**, and then click **Process Definition**.
3. In the **Additional Properties** section, click **Java Virtual Machine**, and then click **Custom Properties**.
4. Click **New** and type the following information:
 - a. In the **Name** field, type `oracle.iam.rm.loader.max_upload_size`.
 - b. In the **Value** field, type the maximum size (in bytes) of data upload that you want to set, for example, `10485760`.

Note: The default value of the maximum size of data upload is 10 MB ($10 \times 1024 \times 1024 = 10485760$). You can modify this value to any other limit.

- c. In the **Description** field, type the description for the maximum upload size that you set, for example, maximum size limit for the Oracle Role Manager loader.
- d. Click **OK**.

4.4.22 Increasing the Transaction Timeout

To increase the transaction timeout:

1. Log in to the WebSphere Administrative Console.
2. In the domain tree, select **Application Servers**, **SERVER_NAME** for example, **server1**.
3. In the **Container Settings** section, expand **Container Service**, and then Click **Transaction Service**.
4. In the **Total transaction lifetime timeout** field, type the new value, 1200, if you want to change the default value, which is 120.
5. In the **Maximum transaction timeout** field, type the new value, 1200, if you want to change the default value, which is 300.
6. Click **Apply** to save the server settings.
7. Restart the server.

Note: For performance tuning of the WebSphere Application Server, refer to the following link:

<http://www-01.ibm.com/software/webservers/appserv/was/performance.html>

4.4.23 Deploying Role Manager Server

To deploy the Role Manager server:

1. Go to **Applications, Install New Application**.
2. Choose **Remote file system**, click **Browse** to navigate to the <ORM_install>/lib directory, select server.ear, and then click **OK**.
3. Click **Next**.
4. On the Map modules to servers page, perform the following substeps:
 - a. From the **Cluster and Servers** list, select the server on which Oracle Role Manager has to be deployed.
 - b. Select both modules, **server.jar** and **ormconsole**.
 - c. Click **Apply**.
 - d. Click **Next**.
5. Click **Finish**.

This could take a few moments to complete.
6. Click **Save**.

To associate the custom user to the Role Manager server:

1. Go to **Applications, Enterprise Applications**.
2. Select **ORM Server**.
3. In the Detail Properties section, click **Security role to user/group mapping**.
4. Select **ORMServer**, and then click **Look up users**.

5. Search and select the **ormserver** user that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29, and move it to the **Selected** list by clicking the right arrow and then click **OK**.
6. In the Security role to user/group mapping page, click **OK**.
7. In the Detail Properties section, click **User RunAs roles**.
8. Perform the following substeps:
 - a. In the **User Name** field, type the User ID that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29.
 - b. In the **password** field, type the password that you created in Step 3 of "[Creating a Custom User](#)" on page 4-29.
 - c. In the **Role(s)** field, select **ORMServer**.
9. Click **Apply**, and then click **OK**.
10. Restart the server on which Role Manager is installed.

Note:

- If you have created a non-admin server in the step 4.4.1 on page 20 for Role Manager, then the non-admin server does not get started automatically when the websphere admin server is started or when the websphere windows service is started. You can start the non-admin server using the following command:

```
[Websphere Profile Install Dir]/bin/startServer.bat
<server-name>
```

- After starting the server on which Role Manager is installed, if you see the status of the Oracle Role Manager Server application through the administrative console of the admin server, it might show as stopped though the application has actually started. You cannot start the application deployed on the non-admin server through the administrative console of the admin server.
-
-

11. To test the server installation, ensure that you can get to the Role Manager administrative console from a Web browser. For example:

```
http://localhost:9080/ormconsole
```

You should be able to see the Home page of the Role Manager administrative console.

4.4.24 Deploying the Role Manager Web Application

To deploy the Role Manager Web application:

1. Go to **Applications, Install New Application**.
2. Select **Remote file system**, click **Browse** to navigate to the `<ORM_install>/webui/websphere/6.1` directory, select `webui.ear`, click **OK** and then click **Next**.
3. On the Select installation options page, accept the defaults and then click **Next**.
4. On the Map modules to servers page, perform the following substeps:

- a. From the **Cluster and Servers** list, select the server on which Oracle Role Manager has to be deployed.
 - b. Select the **webui** module.
 - c. Click **Apply**.
 - d. Click **Next**.
5. Click **Finish**, and then save your changes.
 6. Go to Applications, Enterprise Applications, ORM Web UI.
 7. Click **Manage Modules**.
 8. Click the **webui** link.
 9. In the **Class loader order** list, select **Classes loaded with application class loader first and apply**.
 10. From Applications, Enterprise Applications, select **ORM Web UI**, and then click **Start**.

(This assumes you are administering WebSphere on the same server as the ORM Web UI is installed).

Note: If Web UI is deployed on a non-administrative server, then restart that server.

11. Test the Web application installation as follows:
 - a. In a Web browser, navigate to the Role Manager Web application address. For example:
`http://localhost:9080/webui`
 - b. Log in as the Role Manager Administrator created in the "[Installing Role Manager](#)" on page 3-3 section.
You should be able to see the Home page of the Role Manager Web application.

Loading Data

This chapter provides the information about the following sections:

- [Loading Standard and Sample Data](#)
- [Manual Data Model Deployment](#)

5.1 Loading Standard and Sample Data

To upload the standard data and the sample data into the Role Manager, perform the following procedure.

To load standard and sample data:

1. If the application server on which Role Manager is deployed is not already running, start it.
2. In a Web browser, go to the Role Manager Administrative Console. For example, by default:
JBoss: `http://<host>:8080/ormconsole`
WebSphere: `http://<host>:9080/ormconsole`
WebLogic: `http://<host>:7001/ormconsole`
3. Type user name and password of the Role Manager Administrator previously defined in "[Installing Role Manager](#)" on page 3-3, and then click **Log In**.
4. Click **Upload**.
5. Click **Browse**.
6. Navigate to select the `standard_roles.dar` file found in `<ORM_install>/samples/sample_data`.
7. Click **Load**.
8. Click **refresh** until you see that all processes are finalized.
9. Optionally, to upload sample organizations and people, repeat these steps for the `sample_data.dar` file found in the same location.

Loading the sample data can take several minutes. While data is being loaded, you can click **refresh** to monitor progress.

Once the data load processes display as being finalized, you can go back to the Role Manager Web application and check the sample data.

5.2 Manual Data Model Deployment

If you change the standard configuration or standard data model, you need to run a command to deploy your customizations to the database.

This procedure assumes you have already completed the following steps:

- A database instance has been created for Role Manager with the appropriate tablespaces. (Refer to "Database Setup" on page 3-1.)
- The Role Manager database owner and application user schemas have been created and contain no data. (Refer to "Creating the Role Manager Users" on page 3-3.)
- The database is accessible and the service on which Role Manager is installed is started.

To deploy model and configuration customizations:

1. If you have any custom configuration or data model customizations, create an archive file containing your customizations and append the file name with `.car`. For more information about custom configuration, refer to the "Oracle Role Manager Administrator's Guide" and for more information about data model customization, refer to *Oracle Role Manager Developer's Guide*.
2. In `<ORM_install>/config`, create a file named `db.properties` that contains the following two lines:

```
db.driverClass=oracle.jdbc.driver.OracleDriver
db.connection_string=jdbc:oracle:thin:@$HOST$: $PORT$: $SERVICE_NAME$
```

where `$HOST$` is the database host name, `$PORT$` is the database listener port, and `$SERVICE_NAME$` is the database instance on which the Role Manager users were created.

3. In a command window, navigate to `<ORM_install>/bin`.
4. Run the following command to deploy the configuration and data model and create the Role Manager Administrator:

```
deploy "<collection_of_cars>" <orm-owner> <ormapp-user> <admin-user>
```

where:

`<collection_of_cars>` contains the relative paths and file names of all CAR files to deploy. This collection must be within quotes. This collection must be within quotes with delimiters appropriate to the platform (semicolon (;) for Windows, otherwise colon (:)). If you are not deploying any customized CAR files, the default collection must include `standard.car` and `configurations.car`.

The first deployment must include the `configuration.car*` file. If you require the standard data model, for example, if you want to use the out-of-the-box web UI and/or the sample data, you must also include the `standard.car` file.

Note: The default configuration.car file gives all privileges from the standard data model to the system administrator system role. If you want to start with a more hardened security policy, you must use the configuration_hardened.car file. You can use the hardened configuration and then decide to give privileges set in the default configuration.car file to the system administrator system role. To do so, you can either use the web UI or load the privilege mappings using the admin_systemrole_privilege_mapping.dar file.

<orm-owner> is the username of the Role Manager database owner user created in "[Creating the Role Manager Users](#)" on page 3-3

<ormapp-user> is the username of the Role Manager application user created in "[Creating the Role Manager Users](#)" on page 3-3

<admin-user> is the username for the Role Manager Administrator to create.

5. At the prompt, type the password of the Role Manager database owner.
6. At the prompt, type the password of the Role Manager application user.
7. At the prompt, type the password for the new Role Manager Administrator account.

Note: After deploying the data model and configuration, you must load the sample and the standard data. Refer to "[Loading Standard and Sample Data](#)" on page 5-1 for instructions.

Removing Oracle Role Manager Software

This chapter describes the process of removing Oracle Role Manager software. It contains the following sections:

- [Removing Oracle Role Manager Software](#)
This section describes general instructions for UNIX-based systems and Windows systems.
- [Removing the Oracle Role Manager Database](#)
This section describes specific instructions for dropping the Oracle Role Manager database users/schemas.

6.1 Removing Oracle Role Manager Software

Use the following procedure to uninstall the Oracle Role Manager software:

1. Run the Oracle Universal Installer as follows:

For UNIX-based systems, run the command from `$ORACLE_HOME/oui/bin`:

```
./runInstaller -deinstall -silent REMOVE_HOMES={"$ORACLE_HOME"} from  
$OH/oui/bin
```

For example,

```
$ORACLE_HOME/oui/bin/runInstaller -deinstall -silent  
REMOVE_HOMES={"/scratch/ORMHome_1"}
```

For Windows systems, run the following command from

`$ORACLE_HOME\oui\bin`:

```
setup.exe -deinstall -silent REMOVE_HOMES={"$ORACLE_HOME"} from $OH\oui\bin
```

For example,

```
<ORACLE_HOME>\oui\bin\setup.exe -deinstall -silent REMOVE_HOMES={"C:\orm123"}
```

2. As an alternative for Windows systems, start Oracle Universal Installer from the **Start** menu. On the Welcome page, click **Deinstall Products** to bring up the Oracle Inventory screen.

Select the Oracle home directory and the products that you want to remove by selecting the desired check boxes, then click **Remove**. The Confirmation window appears. Click **Yes** to remove the selected components.

After the Oracle Role Manager components are removed from your system, the **Oracle Inventory** page appears without the removed components. Click **Close** to

close the **Oracle Inventory** page. Click **Cancel** to exit Oracle Universal Installer. Click **Yes** to confirm that you want to exit.

3. Clean up the old Oracle directories.

On systems where Oracle Role Manager is the only Oracle software installed, navigate to the directory for `oracle`, then remove the directory.

For UNIX-based systems, use the `rm -r` command.

Otherwise, delete the Oracle Role Manager home.

For UNIX-based systems, issue the following command to confirm there is no other Oracle home installed.

```
$ grep 'HOME NAME' OraInventory/ContentsXML/Inventory.xml
```

4. Remove the deployments of the Oracle Role Manager server and Web UI from the application server, as appropriate to the application server.

6.2 Removing the Oracle Role Manager Database

Use the following procedure to remove the Oracle Role Manager database:

1. As the Oracle `SYSTEM` user, using `sqlplus` or similar utility, drop the Oracle Role Manager database owner.

2. Check if there are active sessions from users using the following commands:

```
select sid,serial# from v$session where username = 'ORM_DB_OWNER';
select sid,serial# from v$session where username = 'ORM_APP_USER';
```

3. Drop the Oracle Role Manager application user using the following commands:

```
drop user ORM_APP_USER cascade;
drop user ORM_DB_OWNER cascade;
```

4. Drop the Oracle Role Manager tablespaces using the following commands.

```
DROP TABLESPACE ORM_UNDO INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;
DROP TABLESPACE ORM_TEMP INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;
DROP TABLESPACE ORM_INDEX INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;
DROP TABLESPACE ORM_DATA INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;
commit;
```

Manual Configuration of WebLogic Server

This chapter provides the detailed explanation about manual configuration of WebLogic server. Perform these steps only if you intend to configure the WebLogic server manually.

A.1 Overview

This section provides an overview of the manual configuration of WebLogic server:

The section includes:

- [Creating a New Domain](#)
- [Configuring Memory options](#)
- [Configuring Machines](#)
- [Setting Up Commons Logging](#)
- [Configuring Servers](#)
- [Configuring JDBC Data Sources](#)
- [Configuring JMS Messaging Resources](#)
- [Configuring JMS Module Subdeployment](#)
- [Configuring the JMS Connection Factory](#)
- [Configuring a Notification Topic](#)
- [Configuring Queues](#)
- [Configuring Data Upload Size Limit](#)
- [Deploying Role Manager](#)

A.1.1 Creating a New Domain

For Microsoft Windows:

Go to Start, Oracle WebLogic, WebLogic Server 10gR3, Tools, Configuration Wizard for WebLogic 10.3.

For Linux:

1. Go to the WebLogic bin directory using the command:

```
cd BEA_HOME/wlserver_10.3/common/bin for WebLogic 10.3
```

Note: These instructions assume that the installation is a default installation performed with WebLogic server.

2. Start the Configuration Wizard using the following command:

```
sh config.sh
```

3. In the Configuration Wizard:
 - a. Select **Create a New WebLogic domain** and then click **Next**.
 - b. Select **Base this domain on an existing template**. Click **Next**.
 - c. Type the user name and the password, and then confirm the password for the domain. Click **Next**.
 - d. On the left side of the window, select either **Development Mode** or **Production Mode**.

Note: If WebLogic server is configured in production mode, you need to restart the ORMServer to login.

- e. On the right side of the window, select the appropriate JDK and then click **Next**.

Note: If you are using your own JDK, ensure that it is the certified JDK for Oracle WebLogic server.

- f. A message is displayed asking whether you want to customize any of the options mentioned. Select **No**.
 - g. The domain name and domain location are displayed by default. Click **Create**.
 - h. Click **Done**.

A.1.2 Configuring Memory options

To configure memory options:

- For Microsoft Windows systems

Edit the startManagedWebLogic.cmd script and specify memory options as follows:

Follow the format:

```
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
```

Locate the following line:

```
set JAVA_OPTIONS=%JAVA_OPTIONS% -XnoOpt
```

Before this line, add the following if using Sun Java Virtual Machine (JVM):

```
set MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m  
-XX:MaxPermSize=256m
```

Add the following if using JRockit Java Virtual Machine (JVM):

```
set MEM_ARGS=-Xms1280m -Xmx1280m
```

Note: The `-XnoOpt` option turns off adaptive optimization and is required for stable Oracle Role Manager operation.

- For UNIX Systems

Edit the `startManagedWebLogic.sh` script and specify memory options as follows:

Locate the line that starts with the following:

```
$JAVA_HOME/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
```

If using Sun Java Virtual Machine (JVM), add the following line before this line:

```
MEM_ARGS="-Xms1280m -Xmx1280m -XX:PermSize=128m
-XX:MaxPermSize=256m"
```

```
export MEM_ARGS
```

If using JRockit Java Virtual Machine (JVM), add the following line before this line:

```
MEM_ARGS="-Xms1280m -Xmx1280m"
```

```
export MEM_ARGS
```

```
JAVA_OPTIONS="$JAVA_OPTIONS -XnoOpt"
```

```
export JAVA_OPTIONS
```

Note: The `-XnoOpt` option turns off adaptive optimization and is required for stable Oracle Role Manager operation.

A.1.3 Starting WebLogic Server

To start the Oracle WebLogic server:

For Microsoft Windows:

1. For WebLogic 10.3, go to Start, Oracle WebLogic, User Projects, Domain Name, and then click **Start Admin Server for WebLogic Server Domain**.
2. Log on to the WebLogic Server Administration Console by using your new account and by pointing a Web browser to the following URL:

```
http://hostname:7001/console
```

For Linux:

1. Go to the WebLogic `user_projects/domains` directory, for example:

```
cd BEA_HOME/user_projects/domains/
```
2. Go to the directory of the domain that you just created using the Configuration Wizard. For example, `cd domain name`.
3. Start the BEA WebLogic server using the following command:

```
sh startWebLogic.sh
```
4. Log on to the WebLogic Server Administration Console by using your new account and by pointing a Web browser to the following URL:

`http://hostname:7001/console`

A.1.4 Configuring Machines

A machine is a host that runs a WebLogic Server instance. You can configure a machine using the WebLogic Server Administration Console.

To configure a machine:

1. Select **Machines** under Environment and then click **New**.
2. In the **Name** field, type a name for the machine.
3. In the **Machine OS** field, select the operating system.
4. Click **OK**.

To start the node manager:

Use the following steps to start the node manager:

1. Navigate to `WebLogic_install_dir/server/bin`
2. Run the `startNodeManager.cmd` command for Microsoft Windows.
3. Run the `startNodeManager.sh` command for Linux.

A.1.5 Configuring Servers

Note: WebLogic server must be already installed on which Role Manager application is configured.

The server is the machine that hosts the application. Use the following steps to configure a server in the WebLogic Server Administration Console:

To configure a server:

1. Select **Servers** under Environment and then click **New**.
2. In the **Server Name** field, type the name of the Role Manager server, for example `ORMServer`.
3. In the **Server Listen Address** field, type the IP address of the server.
4. In the **Server Listen Port** field, type the Role Manager listening port number .
5. Specify whether the server should belong to a cluster.
6. Click **Next**. Review your choices and then click **Finish**.

To assign a machine to the server:

1. Click the newly created server from the table of servers.
2. Click the **Configuration** tab and then click the **General** subtab.
3. In the **Machine** field, type the machine name.
4. Click **Save**.

To start the server:

1. Select **Servers** under Environment, and then click the newly created server from the table of servers.

2. Click the **Control** tab, then click the **Start/Stop** subtab.
3. Select **ORMServer** and then click **Start**.

A.1.6 Setting Up Commons Logging

Setting up Commons Logging for Oracle Role Manager on WebLogic 10.3 involves creating a new Log4j appender, adding jars to `ORM_WLS_DOMAIN_HOME/lib` and adding `JAVA_OPTION` in `startManagedWebLogic.cmd` for Microsoft Windows and `startManagedWebLogic.sh` for Linux.

To Set Up Commons Logging:

1. Create a new file, `log4j.properties` in `ORM_WLS_DOMAIN_HOME` for example, `BEA_HOME/user_projects/domains/orm_domain`:

```
log4j.rootLogger=debug, ORM

log4j.logger.oracle.iam.rm=debug
log4j.logger.oracle.iam.rm.persistence=INFO
log4j.logger.org.springframework=INFO
log4j.logger.org.apache=WARN
log4j.logger.org.quartz=WARN

# Uncomment all these stdout lines if logs are desired on console
#log4j.appender.stdout=org.apache.log4j.ConsoleAppender
#log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
#log4j.appender.stdout.layout.ConversionPattern=%5p [%d] %t %c (%F:%L) - %m%n
#log4j.appender.stdout.threshold=info

log4j.appender.ORM=org.apache.log4j.RollingFileAppender
log4j.appender.ORM.File=C:/bea/user_projects/domains/orm_domain/servers/ORMServer/logs/ORM.log
# Change the threshold to INFO for less verbose logging
log4j.appender.ORM.threshold=debug
log4j.appender.ORM.MaxFileSize=1024KB
# Keep backup files
log4j.appender.ORM.MaxBackupIndex=5

log4j.appender.ORM.layout=org.apache.log4j.PatternLayout
log4j.appender.ORM.layout.ConversionPattern=%5p [%d] %t %c (%F:%L) - %m%n
```

2. In the file `ORM_WLS_DOMAIN_HOME/bin/startManagedWebLogic.cmd`, add a new line after line 55:

```
@REM. Set JAVA_OPTIONS to the java flags that you want to pass to the vm.
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dlog4j.configuration=file:C:/bea/user_projects/domains/orm_domain/log4j.properties
```

Replace "C:/bea" with `BEA_HOME`.

3. Add the following jars into `ORM_WLS_DOMAIN_HOME/lib` folder:
 - `commons-logging-1.0.4.jar` (download from apache.org)
 - `log4j-1.2.8.jar` (download from apache.org)
4. Restart ORM WebLogic server and you see ORM debug messages in the log-file:

```
BEA_HOME/user_projects/domains/orm_domain/servers/ORMServer
/logs/ORMServer.log
```

A.1.7 Configuring JDBC Data Sources

To configure the non-XA data source:

1. In the Domain tree, select Services, JDBC, Data Sources.
2. Click **New**. The JDBC Data Source Properties page appears.
3. In the **Name** field, type the name of the data source, for example, ORM Data Source.
4. In the **JNDI Name** field, type the JNDI path :
`orm/jdbc/ORMServerDS`
5. From the Database Type list, select **Oracle**.
6. From the Database Driver list, select **Oracle's Driver (Thin)**.
7. Click **Next** and deselect **Supports Global Transactions**.
8. Click **Next**. The Connect Properties page appears.
9. In the **Database Name** field, type the name of the database, for example, (Oracle SID).
10. In the **Host Name** field, type the host name or IP address of the machine hosting the database.
11. In the **Port** field, type the port number on which the database is listening, for example, 1521.
12. In the **Database User Name** field, type the database user name that was created in the Step 3 of the "[Creating the Role Manager Users](#)" on page 3-3 section.
13. In the **Password** field, type the password for the database user and in the **Confirm Password** field, retype the password.
14. Click **Next**. The Test Database Connection page appears.
15. Verify the contents.
16. Click **Next**. The Select Targets page appears.
17. Select **ORMServer** as the target and then click **Finish**.

To configure the XA data source:

1. In the Domain tree, select Services, JDBC, Data Sources.
2. Click **New**. The JDBC Data Source Properties page appears.
3. In the **Name** field, type the name of the data source, for example, ORM XA Data Source.
4. In the **JNDI Name** field, type the JNDI path :
`orm/jdbc/ORMServerXADS`
5. From the Database Type list, select **Oracle**.
6. From the Database Driver list, select **Oracle's Driver (Thin XA)**.
7. Click **Next**.
8. The Transaction Options page appears. Click **Next**.
9. In the **Database Name** field, type the name of the database, for example, (Oracle SID).

10. In the **Host Name** field, type the host name or IP address of the machine hosting the database.
11. In the **Port** field, type the port number on which the database is listening, for example, 1521.
12. In the **Database User Name** field, type the database user name that was created in the Step 3 of the "[Creating the Role Manager Users](#)" on page 3-3 section.
13. In the **Password** field, type the password for the database user and in the Confirm Password field, retype the password.
14. Click **Next**. The Test Connection Database page appears.
15. Verify the contents.
16. Click **Next**. The Select Targets page appears.
17. Select **ORM server** as the target and then click **Finish**.

Note: If you are using RAC database, provide the following string while creating the data source:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1-vip)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2-vip)
(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=orcl.us.oracle.com)))
```

A.1.8 Configuring JMS Messaging Resources

To configure the JMS Server:

1. In the domain tree, select Services, Messaging, JMS Servers.
2. Click **New**. The JMS Server Properties page appears.
3. In the **Name** field, type the name of the Role Manager JMS Server, for example, `ORM JMSServer`.
4. Click **Next**. The Select targets page appears.
5. In the **Target** field, select **ORMServer** as the target and then click **Finish**.

To configure the JMS Module:

1. In the domain tree, select Services > Messaging > JMS Modules.
2. Click **New**. The Create JMS System Module page appears.
3. In the **Name** field, type the name of the Role Manager JMS module, for example, `ORM JMSModule`.
4. Click **Next**. The Target page appears.
5. In the **Target** field, select **ORMServer** as the target and then click **Next**.
6. Click **Finish**.

A.1.9 Configuring JMS Module Subdeployment

To configure JMS Module Subdeployment:

1. In the domain tree, select Services, Messaging, JMS Modules.

2. Click **ORM JMS Module**, for which you want to configure the subdeployment. Click the **Subdeployments** tab.
3. Click **New**. The Subdeployment Properties page appears.
4. In the **Name** field, type the name of the subdeployment, for example, `ORM JMSSubdeployment`.
5. Click **Next**. The Target page appears.
6. Select **ORM JMS Server** as the JMS server target and then click **Finish**.

A.1.10 Configuring the JMS Connection Factory

To configure a JMS Connection Factory:

1. In the domain tree, select Services, Messaging, JMS Modules.
2. Click **ORM JMSModule**.
3. Click **New** under Summary of Resources.
4. Select **Connection Factory** from the list of JMS resources.
5. Click **Next**. The Connection Factory Properties page appears.
6. In the **Name** field, type the name for the connection factory, for example, `ORM ConnectionFactory`.
7. In the **JNDI Name** field, type the path for the connection factory, for example, `orm/jms/ConnFac`.
8. Click **Next** and then click **Finish**.
9. In the domain tree, select Services, Messaging, JMS Modules.
10. Click **ORM JMSModule**.
11. Click **ORM Connection Factory**.
12. Navigate to the **Configuration** tab, **Transactions** sub-tab.
13. Select the **XA Connection Factory Enabled** check box.
14. Click **Save**.

To configure a Finalization Connection Factory:

1. In the domain tree, select Services, Messaging, JMS Modules.
2. Click **ORM JMSModule**.
3. Click **New** under Summary of Resources.
4. Select **Connection Factory** from the list of JMS resources.
5. Click **Next**. The Connection Factory Properties page appears.
6. In the **Name** field, type the name for the connection factory, for example, `Finalization ORM ConnectionFactory`.
7. In the **JNDI Name** field, type the path for the connection factory, for example, `orm/jms/FinalizationConFac`.
8. Click **Next**, and then click **Finish**.
9. In the domain tree, select Services, Messaging, JMS Modules.
10. Click **ORM JMSModule**.

11. Click **Finalization ORM ConnectionFactory**.
12. Navigate to the **Configuration** tab, **Transactions** sub-tab.
13. Select the **XA Connection Factory Enabled** check box.
14. Click **Save**.

A.1.11 Configuring a Notification Topic

To configure a notification topic:

1. In the domain tree, select **Services, Messaging, JMS Modules**.
2. Click **ORM JMS Module**.
3. Click **New** under Summary of Resources.
4. Select **Topic** from the list of JMS resources.
5. Click **Next**. The JMS Destination Properties page appears.
6. In the **Name** field, type a name for the topic, for example, `ORM NotificationTopic`.
7. In the **JNDI Name** field, type the path for accessing the topic, for example, `orm/topic/NotificationTopic`.
8. In the **Template** field, select **None**.
9. Click **Next**.
10. Select **ORM JMSSubdeployment** that you created in the Step 4 of the ["Configuring JMS Module Subdeployment"](#) on page A-8 section from the list.
11. Click **Finish**.

A.1.12 Configuring Queues

To configure the ORM Finisher Queue:

1. In the domain tree, select **Services, Messaging, JMS Modules**.
2. Click **ORM JMS Module**.
3. Click **New** under Summary of Resources.
4. Select **Queue** from the list of JMS resources.
5. Click **Next**. The JMS Destination Properties page appears.
6. In the **Name** field, type a name for the queue, for example, `ORM FinisherQueue`.
7. In the **JNDI Name** field, type the path for accessing the topic as `orm/queue/BtFinisherQueue`.
8. In the **Template** field, select **None**.
9. Click **Next**.
10. Select **ORM JMSSubdeployment** that you created in the Step 4 of the ["Configuring JMS Module Subdeployment"](#) on page A-8 section from the list.
11. Click **Finish**.

To configure the ORM Loader Queue:

1. In the domain tree, select Services, Messaging, JMS Modules.
2. Click **ORM JMS Module**.
3. Click **New** under Summary of Resources.
4. Select **Queue** from the list of JMS resources.
5. Click **Next**. The JMS Destination Properties page appears.
6. In the **Name** field, type a name for the queue, for example, `ORM LoaderQueue`.
7. In the **JNDI Name** field, type the path for accessing the topic as `orm/queue/LoaderQueue`.
8. In the **Template** field, select **None**.
9. Click **Next**.
10. Select **ORM JMSSubdeployment** that you created in the Step 4 of the ["Configuring JMS Module Subdeployment"](#) on page A-8 section from the list.
11. Click **Finish**.

To configure the ORM Incoming Event Queue:

1. In the domain tree, select Services, Messaging, JMS Modules.
2. Click **ORM JMS Module**.
3. Click **New** under Summary of Resources.
4. Select **Queue** from the list of JMS resources.
5. Click **Next**. The JMS Destination Properties page appears.
6. In the **Name** field, type a name for the queue, for example, `ORM IncomingEventQueue`.
7. In the **JNDI Name** field, type the path for accessing the topic as `orm/queue/IncomingEventQueue`.
8. In the **Template** field, select **None**.
9. Click **Next**.
10. Select **ORM JMSSubdeployment** that you created in the Step 4 of the ["Configuring JMS Module Subdeployment"](#) on page A-8 section from the list.
11. Click **Finish**.

A.1.13 Configuring Data Upload Size Limit

You can upload a DAR file to load data of maximum size 10 MB into the system. If you try to load data larger than this maximum upload size limit, you get an error message. You can configure the maximum data upload size limit to a higher or lower value than the default settings.

To configure the data upload size limit:

1. Go to Environment, Servers, ORM Server.
2. On the Configuration tab, click the **Server Start** subtab.
3. In the **Arguments** field, append the following argument to the new value.
`-Doracle.iam.rm.loader.max_upload_size=<new value>`

For example:

```
-Doracle.iam.rm.loader.max_upload_size=1073741824
```

4. Click **Save**.

A.1.14 Creating the Oracle Role Manager User

Before installing the WebLogic server application, you must perform the following steps in the security realm:

1. Go to Security Realms and click the realm name, for example, **myrealm**.
2. Click **Users and Groups** and then **Users**.
3. Click **New** and then type the following details:
 - a. In the **Name** field, type `ormserver`.
 - b. In the **Description** field, type the description, for example, principal that acts as ORM Server.
 - c. In the **Password** field, type the password, for example, `ormserver`.
4. Click **OK**.
5. Click the newly created user, for example, **ormserver**.
6. To add the created user to the Deployers group:
 - a. Go to the **Groups** tab.
 - b. From the Available list, select **Deployers**.
 - c. Click the right-pointing arrow.
 - d. Click **Save**.

A.1.15 Deploying Role Manager

If you have already deployed the Role Manager server earlier and removed it and then try to deploy again, the deployment is delayed. This is because, the error messages related to the previous unsuccessful attempts of installation gets queued up in the log file and delays the deployment procedure. To prevent such delay, perform the following steps before you actually deploy the Role Manager server:

Note: Perform this procedure only if you are repeating the deployment of the same Role Manager server.

1. Start up the Role Manager server that contains the JMS server.
2. Navigate to Services, Messaging, and JMS Modules.
3. Click **ORM JMSModule**.
4. From the resource list, select the **ORMFinisherQueue**.
5. On the Monitoring tab, select the **ORM JMSModule! ORM Finisher Queue** destination and click **Show Messages**.
6. Click **Delete** and from the list of options, select **Delete All**.
7. In the confirmation page, click **Yes**.

To deploy the Role Manager server application:

1. Select **Deployments** in the left part of the Administration Console window.
2. Click **Install** in the right part of the Administration Console window.
3. In the *ORM_HOME*, navigate to the *server.ear* file and select it. Click **Next**.

Note: The *server.ear* file can be accessed from the path *ORACLE_HOME/lib/server.ear*.

4. Select **Install this deployment as an application**. Click **Next**.
5. Select **ORM Server** as the target in the **Target** field. Click **Next**.
6. In the **Name** field, type the name of the Role Manager server application, for example, *ORM ServerApp*.
7. Click **Next** and in the Install Application Client page, click **Finish**.

Note: You must restart the ORMServer to login.

8. Click **Save** to activate the changes.
9. To test the server installation, ensure that you can get to the Role Manager administrative console from a Web browser. For example:

`http://localhost:<port>/ormconsole`

Note: By default 7001 is the port for admin server and 5556 is the port for NodeManager.

You should be able to see the Home page of the Role Manager administrative console.

To start the server application for WebLogic 10.3:

Starting the server application is automatically taken care for WebLogic 10.3.

To deploy the Role Manager Web application:

1. Select **Deployments** in the left part of the Administration Console window.
2. Click **Install** in the right part of the Administration Console window.
3. Navigate to the *webui.war* file and select it. Click **Next**.

Note: The *webui.war* file can be accessed from the path *ORACLE_HOME//webui/weblogic/10.3/webui.war*.

4. Select **Install this deployment as an application**. Click **Next**.
5. In the **Target** field, select **ORMServer** as the target and then click **Next**.
6. In the **Name** field, type the name of the Web user interface application.
7. Select **Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console** from the **Security** list.

-
8. Click **Next** and then click **Finish**.
 9. Test the Web application installation as follows:
 - a. In an Internet Explorer 6 or 7, navigate to the Role Manager Web application address. For example:
`http://localhost:<port>/webui`
 - b. Log in as the Role Manager Administrator created in "[Installing Role Manager](#)" on page 3-3.

Note: Data must be loaded into the system to expose all the functionality of the application. Refer to "[Loading Standard and Sample Data](#)" on page 5-1 for instructions.

You should be able to see the Home page of the Role Manager Web application.

To start the Web application for WebLogic 10.3:

Starting the Web application is automatically taken care for WebLogic 10.3.

Index

A

- activation specifications (AS)
 - authentication, 4-30
 - configuring in WebSphere, 4-27
- administrative account
 - creating at the command line, 5-2
 - creating during installation, 3-5
- administrative console
 - on JBoss, 4-16
- AIX, Oracle Role Manager user account, 3-1
- AS
 - configuring Finisher AS, 4-28
 - configuring Incoming Event AS, 4-27
 - configuring Loader AS, 4-27
 - configuring Notification AS, 4-28
- authentication
 - configuring for J2C connection factories, 4-30
 - configuring for the activation specifications (AS), 4-30

C

- certification, hardware and software, 1-3
- cluster, 4-5
 - nodes, 4-5
- Clustered, 4-5
- configuration, 5-3
- configuration file archives (CAR), 5-2
- connection URL, 4-22, 4-23
- console
 - administrative on JBoss, 4-16
- create-app-user.sql script, 3-3
- create-schema-owner.sql script, 3-3
- create-tablespace.sql script, 3-2
- creating
 - database users, 3-3
 - tablespaces, 3-2

D

- data file archives (DAR), 5-1
- data model
 - manual deployment of, 5-2
 - standard and primordial configuration, 3-4
- data sources

- configuration files for JBoss, 4-15
- creating non-XA data source, 4-22
- creating transaction (XA) data source, 4-23
- data upload
 - size limit, configure, 4-18
- data, loading into Oracle Role Manager, 5-1
- database
 - connection values, 3-5
 - listener port, 2-2
 - split users for security, 3-3
 - synonyms, 3-3
- database alias, creating in WebSphere, 4-22
- database properties file, for manual deployment and other commands, 5-2
- database users, creating, 3-3
- deploy command, 5-2

F

- finalization bus, changing name of, 4-24
- Finisher activation specifications (AS), 4-28
- Finisher Queue (finalization), 4-27
- Finisher Queue bus destination, 4-25

H

- hardware and software certifications, 1-3
- host requirements
 - Oracle Role Manager Application Server, 2-1
 - Oracle Role Manager Database Server, 2-1

I

- Incoming Event activation specifications (AS), 4-27
- Incoming Event Queue, 4-26
- Incoming Event Queue bus destination, 4-25
- init.ora, modifying, 3-3
- installation
 - manual deployment of configuration, 5-2
 - noninteractive, 3-6
 - overview, 1-2
 - server test on JBoss, 4-16
 - Web application test on JBoss, 4-16
 - worksheet, 2-2
- integration with Oracle Identity Manager, data model configuration, 3-5

J

- J2C connection factories, authentication for, 4-30
- JBoss configuration, 4-1
- JDBC
 - non-XA, 4-22
 - transaction (XA) configuration, 4-20
- JDBC connection URL, 4-22, 4-23
- JDBC data sources
 - creating non-XA data source, 4-22
 - creating transaction (XA) data source, 4-23
- JDBC drivers, path to, 4-21
- JDBC providers
 - creating for non-XA data source, 4-21
- JMS configuration file for JBoss, 4-15
- JMS messaging buses
 - adding servers to, 4-24
 - changing the name of, 4-24
 - configuring destinations, 4-25
 - for finalization, 4-24
 - for Oracle Role Manager, 4-24
- JMS queue connection factories, 4-25
- JMS queues
 - configuring Finisher Queue (finalization), 4-27
 - configuring Incoming Event Queue, 4-26
 - configuring Loader Queue, 4-26
 - configuring Notification Topic Queue, 4-27, 4-28
- JMS topic connection factory, 4-26
- JNDI names
 - for Finisher AS, 4-28
 - for Finisher Queue (finalization), 4-27
 - for Incoming Event AS, 4-27
 - for Incoming Event Queue, 4-26
 - for Loader AS, 4-27
 - for Loader Queue, 4-26
 - for non-XA data source, 4-22
 - for Notification AS, 4-28
 - for Notification Topic Queue, 4-27, 4-28
 - for Oracle Role Manager Finalization queue connection factory, 4-26
 - for Oracle Role Manager queue connection factory, 4-25
 - for transaction (XA) data source, 4-23

L

- Linux, Oracle Role Manager user account, 3-1
- load standard and sample data, 5-1
- Loader activation specifications (AS), 4-27
- Loader Queue, 4-26
- Loader Queue destination bus, 4-25
- loading data into Oracle Role Manager, 5-1

M

- manual configuration of WebLogic server, A-1
- maximum connections
 - setting for the non-XA data source, 4-23
 - setting for the transaction data source, 4-24
- memory options
 - unix, A-3

Index-2

- windows, A-2
- multiple Oracle homes, 1-3

N

- non-XA configuration, 4-22
- non-XA data source, 4-22
 - JNDI name, 4-22
 - setting maximum connections, 4-23
- non-XA JDBC provider, 4-21
- Notification activation specifications (AS), 4-28
- Notification Topic bus destination, 4-25
- Notification Topic Queue, 4-27, 4-28

O

- Oracle homes, multiple, 1-3
- Oracle Role Manager
 - base directory, 2-2
 - creating users/schemas, 3-3
 - database alias in WebSphere, 4-22
 - JMS buses, 4-24
 - JNDI names, 4-22, 4-23
 - tablespaces, 3-2
- Oracle Role Manager Administrator
 - creating at the command line, 5-2
 - creating during installation, 3-5
- Oracle Role Manager user account on UNIX-based systems, 3-1
- ORM bus, 4-24
- orm-ds.xml file, 4-15
- orm.rsp response file, 1-1
- orm-service.xml file, 4-15

P

- primordial data model, 3-5

Q

- queue connection factories
 - for Oracle Role Manager, 4-25
 - for Oracle Role Manager Finalization, 4-25

R

- response file template, 1-1, 3-6
- rollback segments, configuring, 3-2

S

- sample data, loading into Oracle Role Manager, 5-1
- schemas, creating, 3-3
- securing message bus, 4-31
- security, split database users for security, 3-3
- server.ear file
 - deploying in JBoss, 4-16
 - deploying in WebSphere, 4-32, 4-33
- servers, adding to JMS messaging buses, 4-24
- silent installation, 1-1, 3-6
- single sign-on, 1-3

software and hardware certifications, 1-3

T

tablespaces

- creating, 3-2

- using alternate, 3-3

testing Oracle Role Manager application installation

- on JBoss, 4-16

testing Oracle Role Manager server installation

- on JBoss, 4-16

transaction data source, 4-23

- JNDI name, 4-23

- setting maximum connections, 4-24

W

WebLogic

- cluster, 4-5

WebLogic server, configure, 4-1

WebSphere

- transaction timeout, 4-32

WebSphere configuration, 4-18

WebSphereFinalizationBusName property, 4-24

webui.war file

- deploying in JBoss, 4-16

worksheet, 2-2

X

XA data source, 4-23

- JNDI name, 4-23

- setting maximum connections, 4-24

