Oracle® Fusion Middleware

Deployment Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.3.0)

E57637-03

October 2016

Documentation for system administrators that describes how to use the Identity and Access Management Deployment Wizard and related tools to deploy Oracle Identity and Access Management components for Oracle Fusion Middleware.

ORACLE

Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.3.0)

E57637-03

Copyright © 2014, 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Shynitha Shanthakumar

Contributing Authors: Rajesh Gouthaman, Wortimla RS

Contributors: Nagasravani Akula, Alen Alex, Niranjan Ananthapadmanabha, Jeremy Banford, Javed Beg, John Boyer, Guruaj BS, Lancer Guo, Simon Kissane, Manohari Neelakanteshwari, Rob Otto, Mehul Poladia, Anupama Pundpal, Jatan Rajvanshi, Michael Rhys, Avani Shah, Kopal Sinha, Sandeep Suthari, Vaibhav Tiwari, Sandeep Reddy Vinta, Norman Wang, Amy Yue, Warren Zheng, Peter LaQuerre

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface vii

Audience vii
Documentation Accessibility vii
Related Documents vii
Conventions vii

1 Introduction to the Life Cycle Management (LCM) Tools

1.1 About the Automated Deployment of Oracle Identity and Access Management 1-1
1.1.1 Purpose of the Automation Tools for 11*g* Release 2 (11.1.2.3) 1-1
1.1.2 Packaging and Distribution of the Automation Tools 1-2
1.1.3 Deployment Capabilities of the LCM Tools for Oracle Identity and Access Management 1-2
1.1.4 Patching Capabilities of the LCM Tools for Oracle Identity and Access Management 1-3
1.1.5 Upgrade Capabilities of the LCM Tools for Oracle Identity and Access Management 1-4
1.2 Overview of Deploying Oracle Identity and Access Management With the LCM Tools 1-4
1.3 Oracle Identity and Access Management Topologies Supported by the LCM Tools..... 1-5
1.3.1 Diagram of the OIM-Only Topology 1-6
1.3.2 Diagram of the Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS) Only Topology 1-6
1.3.3 Diagram of the OIM-OAM-OMSS Integrated with Directory Topology 1-7
1.4 Understanding the Supported Oracle Identity Manager Topologies 1-8
1.4.1 About the Web Tier 1-8
1.4.2 About the Application Tier 1-9
1.4.3 About the Directory/Database Tier 1-9

2 Installing and Preparing to Use the Life Cycle Management Tools

2.1 Verifying Certification, System Requirements, and Interoperability..... 2-1
2.2 Running the Health Check Utility to Verify Basic System Requirements..... 2-2
2.2.1 Understanding the Oracle Identity and Access Environment Health Check Utility. 2-2
2.2.2 Running the Environment Health Check Utility Before Installing the LCM Tools... 2-3
2.3 Understanding the Directory Server Requirements for Oracle Identity Management 2-4
2.3.1 What LDAP Directories Are Supported by Oracle Identity Management?..... 2-4
2.3.2 What Topologies Require an LDAP Directory? 2-4
2.3.3 How Do I Prepare an Existing LDAP Directory for Oracle Identity Management ... 2-4

2.4 Obtaining the LCM Tools and Oracle Identity Management Software Repository..... 2-5
2.5 About the Deployment Repository and LCM Tools Directory Structure..... 2-5
2.6 About Preparing a Database for an Oracle Identity Management Deployment..... 2-6
2.7 Locating the Required Java Development Kit (JDK)..... 2-7
2.8 Installing the Oracle Identity Management Lifecycle Tools..... 2-7
2.8.1 Locating and Starting the LCM Tools Installer..... 2-7
2.8.2 Summary of the LCM Tools Installer Screens..... 2-8
2.8.3 Specifying an Inventory Directory..... 2-8
2.9 Applying Patches and Workarounds..... 2-9
2.9.1 Mandatory Patches Required for Installing Oracle Identity Manager..... 2-10
2.10 Optionally Running Repository Creation Utility (RCU) to Create the Required Schemas..... 2-11
2.10.1 Locating and Starting RCU to Prepare for an Automated Deployment..... 2-11
2.10.2 Using RCU to Install the Required Oracle Identity Management Schemas..... 2-11
2.10.2.1 Considerations When Using RCU to Install the Schemas for an Automated Deployment 2-12
2.10.2.2 Selecting the Required Schemas for Supported Automated Installation Topologies 2-12

3 Preparing an Existing Directory Service for Oracle Identity and Access Management

3.1 Preparing an Existing OUD or OID Directory Service for Use with an Automated Oracle Identity and Access Management Deployment 3-1
3.1.1 About the idmConfigTool_STA Script..... 3-1
3.1.2 Setting up Environment Variables to Run the idmConfigTool_STA Script..... 3-2
3.1.3 Editing the Properties File for the idmConfigTool_STA Script..... 3-2
3.1.4 Preparing a Password File..... 3-3
3.1.5 Running the preConfigIDStore Command..... 3-3
3.1.6 Running the prepareIDStore Command..... 3-4
3.1.7 Ensuring the Success of Running idmConfigTool..... 3-4
3.2 Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management 3-5
3.2.1 Adding the Required Schemas to the Active Directory Instance..... 3-5
3.2.2 Creating the Required Containers in the Active Directory Instance..... 3-6
3.2.3 Adding Access Control Lists (ACLs) to the Containers in Active Directory..... 3-8
3.2.4 Creating Users in the Active Directory Instance..... 3-9
3.2.5 Adding User Memberships to Groups in an Active Directory Instance..... 3-11
3.2.5.1 Summary of the Groups and Users for an OAM and OMSS Deployment..... 3-11
3.2.5.2 Summary of the Groups and Users for an Integrated OIM, OAM, and OMSS Deployment 3-11
3.2.6 Assigning Administrator Privileges to the OIMAdministrators Group..... 3-12
3.2.7 Resetting User Passwords in an Active Directory Instance..... 3-12
3.2.8 Enabling User Accounts for in an Active Directory Instance..... 3-12
3.2.9 Setting the LockoutThreshold in Active Directory..... 3-13
3.3 Configuring Active Directory in SSL Mode..... 3-13

4 Creating a Deployment Response File

4.1 What is a Deployment Response File? 4-1
4.2 Starting the Deployment Wizard and Navigating the Common Screens 4-1
4.3 Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology 4-3
4.4 Creating a Deployment Response File for an Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Topology 4-5
4.5 Creating a Deployment Response File for an Integrated OIM, OAM, and OMSS Topology .. 4-8
4.6 Additional Information When Creating a Response File for an Automated Deployment 4-13
4.6.1 How To Specify the Installation and Configuration Locations in the Deployment Wizard 4-13
4.6.2 Tips When Providing Database Connection Details in the Deployment Wizard .. 4-14
4.6.3 Tips When Providing Directory Service Information in the Deployment Wizard . 4-14

5 Performing Oracle Identity and Access Management Deployment

5.1 Understanding the Stages of an Oracle Identity Management Automated Deployment 5-1
5.2 About the Services and Servers Configured in Each Deployment Phase..... 5-5
5.3 Manual Deployment Tasks When Using Microsoft Active Directory for an Integrated Topology 5-7
5.3.1 Extending the OIM Schema for Active Directory After the Install Phase 5-7
5.3.2 Disabling the LDAPAddMissingObjectClasses Event Handler After the Configure Phase 5-8
5.4 Running the Environment Health Check Utility Before Deployment 5-8
5.5 Deploying Oracle Identity and Access Management Using the LCM Tools 5-9
5.5.1 Deploying Oracle Identity and Access Management Using the Deployment Wizard..... 5-9
5.5.2 Deploying Oracle Identity and Access Management Using the LCM Tools Command Line 5-11
5.6 Reviewing Environment Health Check Utility Reports and Logs After Deployment .. 5-12

6 Post Deployment Tasks

6.1 Post Deployment Task for Accessing Help on the WebLogic Administration Console .. 6-1
6.2 Starting and Stopping Oracle Identity and Access Management Components After an Automated Deployment 6-2
6.2.1 Starting and Stopping Components Using the Provided Start and Stop Scripts 6-2
6.2.1.1 Locating the Provided Start and Stop Scripts..... 6-2
6.2.1.2 About Password Management When Using the Start and Stop Scripts 6-2
6.2.1.3 Starting Components Using the Provided Scripts..... 6-3
6.2.1.4 Stopping Components Using the Provided Scripts..... 6-3
6.2.1.5 Optional Arguments When Using the Start and Stop Scripts..... 6-3
6.2.1.6 Changing the Passwords in the credconfig Wallet..... 6-4
6.2.2 Starting and Stopping Components Manually..... 6-4
6.2.2.1 Understanding the Required Order of Starting and Stopping Components..... 6-5
6.2.2.2 Getting General Information About Starting and Stopping Oracle Fusion Middleware Components 6-5

7 Validating Deployment

7.1 Verifying Connectivity to the Administration Server 7-1
7.1.1 Verifying the Administration Server Connectivity for Oracle Access Management 7-1
7.1.2 Verifying Administration Server Connectivity for Oracle Identity Manager 7-2
7.2 Validating the Access Manager and Oracle Mobile Security Manager Configuration 7-2
7.3 Validating Oracle Identity Manager 7-2
7.4 Validating WebGate and the Access Manager Single Sign-On Setup..... 7-3

8 Troubleshooting Oracle Identity and Access Management Deployment

8.1 Getting Started with Troubleshooting 8-1
8.1.1 Using the Log Files 8-1
8.1.2 Recovering From Oracle Identity and Access Management Deployment Failure..... 8-2
8.2 Using My Oracle Support for Additional Troubleshooting Information 8-2

A Cleaning Up an Environment Before Rerunning IAM Deployment

A.1 About the Cleanup and Restore Feature A-1
A.1.1 Directories Affected by Cleanup and Restore A-1
A.1.2 Where Does Cleanup and Restore Save Its Data? A-2
A.1.3 About Managing Schemas When You Use Cleanup and Restore A-2
A.1.4 Performing Cleanup and Restore Using the Command Line Deployment Tool A-2
A.1.4.1 Using the Command Line to Clean Up a Failed Deployment A-2
A.1.4.2 Using the Command Line to Restore the Install Phase Content A-3
A.1.5 Performing Cleanup and Restore Using the Identity and Access Management Deployment Wizard A-4
A.2 Manual Cleanup of Environment A-4

Preface

This guide describes how to use the new Oracle Identity and Access Management Deployment Wizard and related tools.

Audience

The *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management* is intended for administrators who are responsible for installing and configuring a simple, single host Oracle Identity and Access Management topology.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware documentation set:

- *Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Patching Guide for Oracle Identity and Access Management*

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.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Planning for an Automatic Deployment of Oracle Identity and Access Management

Part I provides an introduction to Oracle Identity and Access Management Deployment. It provides information about the deployment topologies and deployment concepts. It also covers information about the preparatory tasks, and prerequisites for deploying Oracle Identity and Access Management.

Part I contains the following chapters:

- Chapter 1, "Introduction to the Life Cycle Management (LCM) Tools"
- Chapter 2, "Installing and Preparing to Use the Life Cycle Management Tools"
- Chapter 3, "Preparing an Existing Directory Service for Oracle Identity and Access Management"

1

Introduction to the Life Cycle Management (LCM) Tools

This chapter describes and illustrates the deployment reference topologies you can deploy using the Life Cycle Management (LCM) tools and the instructions in this guide. It also summarizes the high-level tasks required to install and deploy the Oracle Identity and Access Management software using the LCM tools.

This chapter contains the following sections:

- Section 1.1, "About the Automated Deployment of Oracle Identity and Access Management"
- Section 1.2, "Overview of Deploying Oracle Identity and Access Management With the LCM Tools"
- Section 1.3, "Oracle Identity and Access Management Topologies Supported by the LCM Tools"
- Section 1.4, "Understanding the Supported Oracle Identity Manager Topologies"

1.1 About the Automated Deployment of Oracle Identity and Access Management

The following sections describe the Oracle Identity and Access Management automated deployment, patching, and upgrade tools:

- Section 1.1.1, "Purpose of the Automation Tools for 11g Release 2 (11.1.2.3)"
- Section 1.1.2, "Packaging and Distribution of the Automation Tools"
- Section 1.1.3, "Deployment Capabilities of the LCM Tools for Oracle Identity and Access Management"
- Section 1.1.4, "Patching Capabilities of the LCM Tools for Oracle Identity and Access Management"
- Section 1.1.5, "Upgrade Capabilities of the LCM Tools for Oracle Identity and Access Management"

1.1.1 Purpose of the Automation Tools for 11*g* Release 2 (11.1.2.3)

The LCM tools provide automated installation and configuration capabilities for Oracle Identity and Access Management on both single host environments and on highly available, production systems.

Use this guide to automate the deployment of Oracle Identity and Access Management on a single host, primarily for evaluation of the Oracle Identity and Access Management software.

For information about using the LCM tools to deploy Oracle Identity and Access Management in a highly available production environment, refer to the *Enterprise Deployment Guide for Oracle Identity and Access Management*.

You can use the LCM tools as an alternative to the manual installation and configuration steps provided in the *Installation Guide for Oracle Identity and Access Management*.

1.1.2 Packaging and Distribution of the Automation Tools

Oracle packages all the software required to automatically deploy, patch, and upgrade Oracle Identity and Access Management in a single software distribution known as the Oracle Identity and Access Management Deployment Repository.

When you download and unpack the archives for Deployment Repository distribution, you end up with a directory structure that contains a software repository. Within this repository are all the software installers required to install and configure Oracle Identity Manager, as well as the Oracle Identity and Access Management Life Cycle Management Tools.

For more informations, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

1.1.3 Deployment Capabilities of the LCM Tools for Oracle Identity and Access Management

The LCM tools for Oracle Identity and Access Management provide the following deployment capabilities and restrictions:

- The Oracle Identity and Access Management LCM tools automate all aspects of installing, configuring, deploying, and patching the software.

  Note however, that this guide describes a limited number of specific Oracle Identity and Access Management topologies on a single host. For more information about the topologies supported by this guide, see Section 1.3, "Oracle Identity and Access Management Topologies Supported by the LCM Tools".

  For additional topologies, see the *Enterprise Deployment Guide for Oracle Identity and Access Management*.

- The Oracle Identity and Access Management software and the required components such as the Java Development Kit (JDK), Oracle WebLogic Server, Oracle HTTP Server, and Oracle SOA Suite are packaged into a single repository that can be downloaded from the Oracle Technology Network (OTN) or the Oracle Software Delivery Cloud.

  This single repository makes it easy to be sure you have the correct prerequisite software before you begin the deployment process. This repository includes a set of software installers and is a completely different download from the conventional distributions available for the standard, manual installation process.

- If the LCM tools are used to deploy Oracle HTTP Server with the Oracle Access Manager Webgate software, then the Webgate will be configured to automatically protect relevant Oracle Identity and Access Management management consoles.

- The LCM Tools use the Environment Health Check Utility to verify that your system requirements before you deploy and to verify the environment after you deploy.

  For more information, see *Verifying Your Oracle Identity and Access Management Environment*.

- The environment you deploy using the LCM tools can later be upgraded component by component, so as to minimize downtime.

  Further, in an integrated environment, where the automated tools are used to deploy multiple Oracle Identity and Access Management products, you can choose to upgrade one product without affecting other products.

  For more information, see the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.

1.1.4 Patching Capabilities of the LCM Tools for Oracle Identity and Access Management

You can use the LCM tools to apply one or more Interim (one-off) or Bundle Patches to an IDM deployment that was installed using the LCM tools. It is important to note that automated patching is supported only for those components installed and configured using the LCM tools.

All patching occurs within a patch session. Each Oracle Identity and Access Management deployment topology is implemented as multiple tiers, including the Directory tier, Application tier, and Web tier. Each product belongs to a single tier, but common patches, if found, are applied to all three.

A session can be created to apply one or more patches, or to rollback selected patches. A session in progress can be aborted if required. If actions need to be rolled back, in the current tier or for tiers that have already been completed, a new rollback session can be created using patches for the affected products.

When patching an environment that was created with the LCM tools, the LCM patching feature:

- Patches all nodes
- Applies the patch to both shared and local storage
- Stops and starts affected servers
- Executes post-patch artifact changes
- Provides comprehensive state-sharing and reporting

Note: Automated patching does *not* support the following:

- Patching of the database and Oracle WebLogic Server
- Patching of Oracle Access Manager Webgates used for Web servers
- Patching of the LCM Tools

For more information about the patching capabilities of the LCM tools, see "Patching Oracle Identity and Access Management Using Lifecycle Tools" in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*

1.1.5 Upgrade Capabilities of the LCM Tools for Oracle Identity and Access Management

For environments that were created using the LCM tools, the upgrade to a newer Oracle Identity and Access Management release is also automated.

To upgrade such an environment, you download a set of upgrade scripts, which can be customized to recognize the details of your environment. The scripts automate all the steps involved with upgrading an Oracle Identity Manager environment that was created using the LCM tools.

As with automated patching, the automated tools do not upgrade the database, JDK, or Webgate software. It does, however, upgrade the Oracle HTTP Server instances that were deployed using the LCM tools.

For more information, see the "Upgrading Oracle Identity and Access Management LCM Provisioned Environments" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.

1.2 Overview of Deploying Oracle Identity and Access Management With the LCM Tools

Table 1–1 describes each of the steps and provides links to more information about each step.

Table 1–1 Roadmap for Creating the Reference Topologies with the LCM Tools

Task	Description	More Information
Determine the topology you want to deploy	Review the topologies supported by the LCM Tools and determine which topology is best suited for the requirements of your organization.	Section 1.3, "Oracle Identity and Access Management Topologies Supported by the LCM Tools"
Review the certifications and system requirements.	Before you install and configure Oracle Identity and Access Management, you should ensure that your existing products are certified for use with Oracle Identity and Access Management. In addition, you should review the system requirements, such as memory and disk space requirements and required Linux install packages.	Section 2.1, "Verifying Certification, System Requirements, and Interoperability"
Run the Health Check Utility to ensure your certification and system requirements have been met.	This step ensures that you can run the Deployment Wizard and the basic and mandatory system requirements have been met.	Section 2.2, "Running the Health Check Utility to Verify Basic System Requirements"
Determine the LDAP Directory requirements for the topology you selected	Some of the supported topologies require a supported LDAP directory service. If you plan to use an existing directory service, there are tasks you must perform to prepare the directory for use with Oracle Identity and Access Management.	Section 2.3, "Understanding the Directory Server Requirements for Oracle Identity Management"

Table 1–1 (Cont.) Roadmap for Creating the Reference Topologies with the LCM Tools

Task	Description	More Information
Download and unpack the LCM Tools and Repository from the Oracle Technology Network (OTN) or the Software Delivery Cloud	When you unpack the archives, you end up with a standard directory structure that includes a software repository. The software repository contains all the installers required to install the Oracle Identity and Access Management software, as well as the installer for installing the LCM Tools.	Section 2.4, "Obtaining the LCM Tools and Oracle Identity Management Software Repository"
Identify and prepare a database for use with Oracle Identity and Access Management	A database is required to store the required schemas for the Oracle Identity and Access Management products and components. You can identify an existing database instance, or use the database installation software included in the repository to install a new database.	Section 2.6, "About Preparing a Database for an Oracle Identity Management Deployment"
Install the LCM Tools	From the software repository, locate and run the LCM Tools installer, which installs the provisioning tools that enable you to automatically deploy Oracle Identity and Access Management.	Section 2.8, "Installing the Oracle Identity Management Lifecycle Tools"
Run the Deployment Wizard to create a new deployment response file.	The Deployment Wizard (one of the LCM Tools), prompts you for important information about your hardware and software environment, such as the selected topology, database, and LDAP directory information. The wizard uses this information to create a response file that can later be used to automatically deploy Oracle Identity and Access Management.	Chapter 4, "Creating a Deployment Response File"
Run the Deployment Wizard or the command line to deploy the Oracle Identity Manager software.	For this step, you use the response file (which now contains all the details about your hardware and software environment) to deploy the Oracle Identity and Access Management software automatically.	Chapter 5, "Performing Oracle Identity and Access Management Deployment"

1.3 Oracle Identity and Access Management Topologies Supported by the LCM Tools

This section describes the reference topologies you can create using the Oracle Identity and Access Management LCM Tools. This guide provides complete instructions for creating this topology with the Oracle Identity and Access Management LCM Tools.

For more information, refer to the following topics:

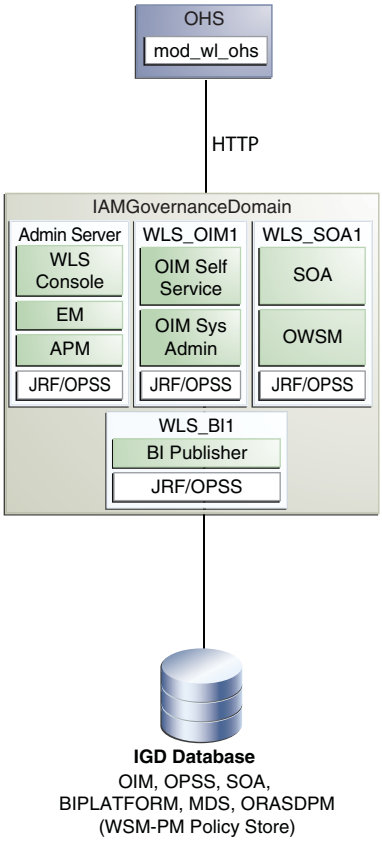
- Section 1.3.1, "Diagram of the OIM-Only Topology"
- Section 1.3.2, "Diagram of the Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS) Only Topology"

- Section 1.3.3, "Diagram of the OIM-OAM-OMSS Integrated with Directory Topology"

1.3.1 Diagram of the OIM-Only Topology

Figure 1–1 shows the topology you can create by selecting the **Oracle Identity Manager (OIM) Only** option on the Select IAM Products page in the Oracle Identity Manager Deployment Wizard.

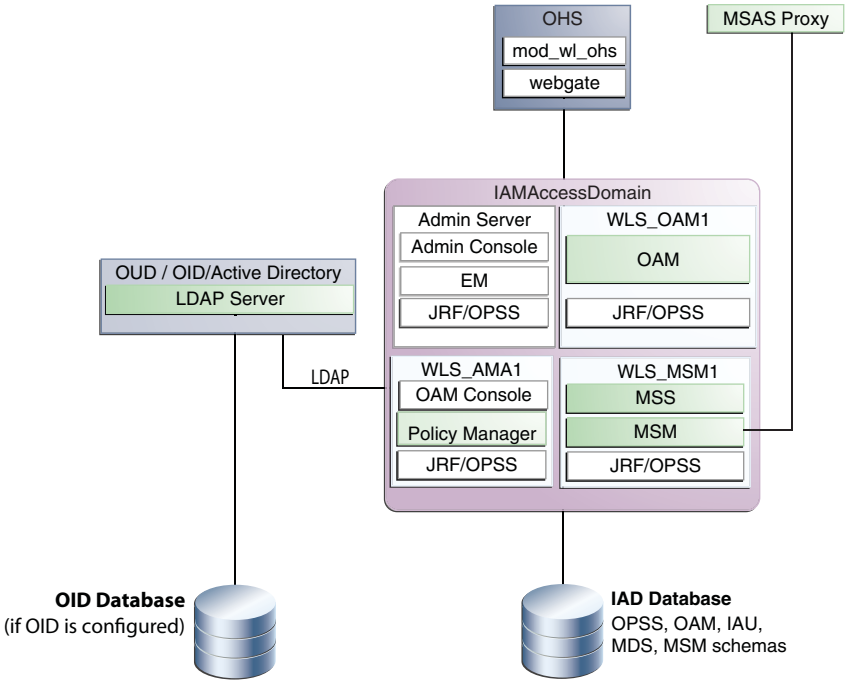
Figure 1–1 Oracle Identity Manager (OIM) Only Topology Diagram



1.3.2 Diagram of the Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS) Only Topology

Figure 1–2 shows the topology you can create by selecting the **Oracle Access Manager (OAM) Suite and Oracle Mobile Suite (OMSS) Only** option on the Select IAM Products page in the Oracle Identity and Access Management Deployment Wizard.

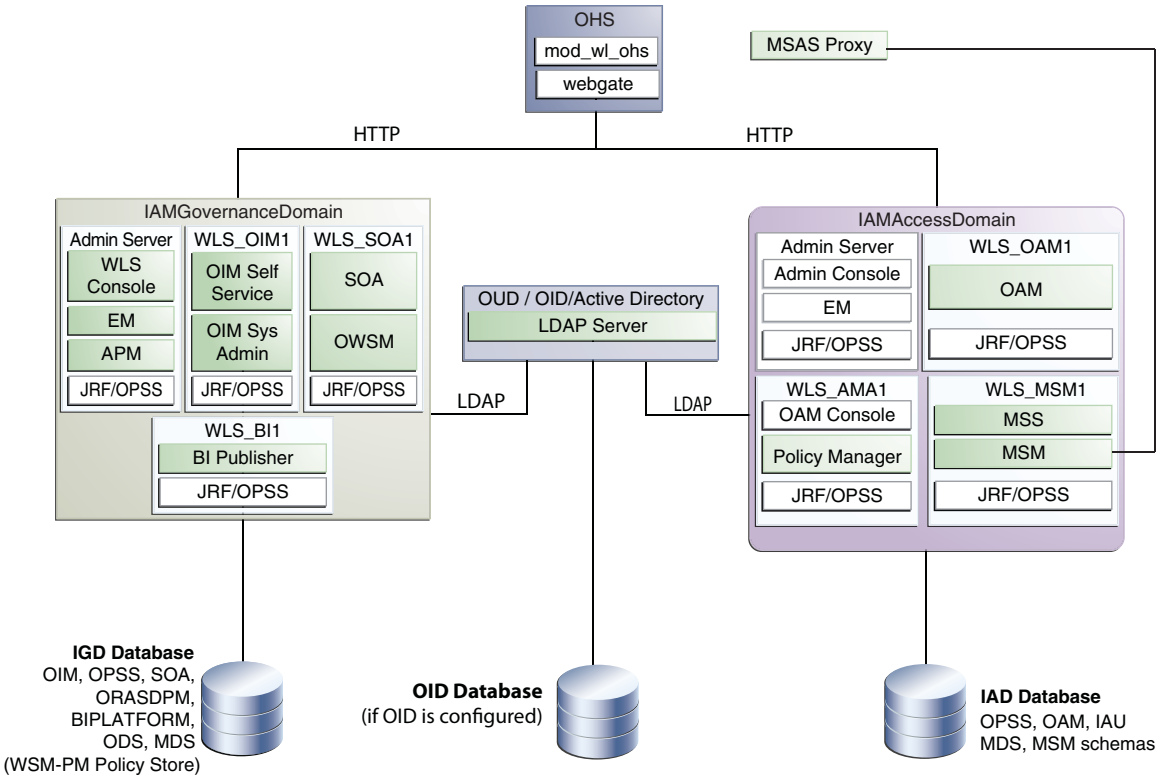
Figure 1–2 Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS) Only Topology Diagram



1.3.3 Diagram of the OIM-OAM-OMSS Integrated with Directory Topology

Figure 1–3 shows the topology you can create by selecting the **OIM-OAM-OMSS Integrated with Directory Only** option on the Select IAM Products page in the Oracle Identity and Access Management Deployment Wizard.

Figure 1–3 OIM-OAM-OMSS Integrated with Directory Topology



1.4 Understanding the Supported Oracle Identity Manager Topologies

Each of the topologies supported by the LCM Tools can be organized into three tiers, as a way to explain the purpose and structure of the topology elements:

- Web Tier
- Application Tier
- Directory/Database Tier

Although it is not shown on the figures, there can also be a directory tier (which is often included in the database tier). If a dedicated directory tier is introduced, LDAP directories can be placed within that tier.

This section contains the following topics:

- Section 1.4.1, "About the Web Tier"
- Section 1.4.2, "About the Application Tier"
- Section 1.4.3, "About the Directory/Database Tier,"

1.4.1 About the Web Tier

Most of the Identity and Access Management components can function without the web tier, but for most enterprise deployments, the web tier is desirable. For example, to support enterprise level single sign-on using products such as Oracle Single Sign-On and Access Manager, the web tier is required.

In the web tier, Oracle HTTP Server, WebGate (an Access Manager component), and the `mod_wl_ohs` plug-in module are installed. The `mod_wl_ohs` plug-in module enables

requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.

The web tier also is where the Mobile Security Access Server (MSAS) is installed when you select any topology that includes Oracle Access Manager. MSAS is a component in the Oracle Mobile Security Suite that provides a central access point for securing traffic from mobile devices to intranet resources. For more information, see "Mobile Security Access Server Architecture Overview" in *Administering Oracle Mobile Security Access Server*.

1.4.2 About the Application Tier

Depending on the topology you are deploying, the application tier can consist of the following Oracle Identity and Access Management components:

- Oracle Access Management Access Manager (OAM) and its related components, deployed in the IAMAccess domain. Within this domain:
  - The Oracle WebLogic Server Administration Server hosts the Oracle WebLogic Server Administration Console, and Oracle Enterprise Manager Fusion Middleware Control.
  - A set of Managed Servers configured with Oracle JRF, which provides the frameworks and infrastructure for the Oracle Fusion Middleware software
  - The WLS_OAM1 Managed Server, which hosts the Oracle Access Manager J2EE application.
  - The WLS_AMA1 Managed Server, which hosts Access Management Administration software, including the Policy Manager and the Oracle Access Manager Console.
  - The WLS_MSM1 Managed Server, which hosts the Oracle Mobile Security Services sofware. Mobile devices can then be configured to use a proxy that connects to the Mobile Security Access Server, running on the WLS_MSM Managed Server.
- The governance components, which are deployed to the IAMGovernence domain. Within this domain:
  - The Oracle WebLogic Server Administration Server for the domain hosts the Oracle WebLogic Server Administration Console, Oracle Enterprise Manager Fusion Middleware Control, and the Oracle Access Manager Console.
  - A set of Managed Servers configured with Oracle JRF, which provides the frameworks and infrastructure for the Oracle Fusion Middleware software
  - The WLS_OIM1 Managed Server, which hosts the Oracle Identity Manager self-service console and Oracle Identity Manager system administration software.
  - The WLS_SOA1 Managed Server, which hosts Oracle SOA Suite and Oracle Web Services Manager (OWSM).
  - The WLS_BI1 Managed Server, which hosts the Oracle Business Intelligence Publisher sofware, which is automatically configured for use with Oracle Identity Manager during deployment.

1.4.3 About the Directory/Database Tier

The database tier consists of:

- One or more databases where the required product schemas are installed. The schemas installed depend up on which components are configured as part of the topology.

  For an Oracle Access Manager deployment, the database is referred to as the IAD Database; for an Oracle Identity Manager deployment, it's referred to as the IGD Database.

- An LDAP directory service (LDAP Server), which is preconfigured before deployment for use with Oracle Access Manager, or with LDAP sync when Oracle Identity Manager and Oracle Access Manager are deployed as part of an integrated topology.

  This directory can be an Oracle Unified Directory, Oracle Internet Directory, or a Microsoft Active Directory Instance. If it is an Oracle Internet Directory instance, you can use a separate database for the Oracle Internet Directory data.

2

Installing and Preparing to Use the Life Cycle Management Tools

This chapter describes the prerequisites for deploying Oracle Identity and Access Management.

Before deploying Oracle Identity and Access Management using the Oracle Identity and Access Management Deployment Wizard, you must complete all prerequisites described in this section.

This chapter contains the following sections:

- Section 2.1, "Verifying Certification, System Requirements, and Interoperability"
- Section 2.2, "Running the Health Check Utility to Verify Basic System Requirements"
- Section 2.3, "Understanding the Directory Server Requirements for Oracle Identity Management"
- Section 2.4, "Obtaining the LCM Tools and Oracle Identity Management Software Repository"
- Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure"
- Section 2.6, "About Preparing a Database for an Oracle Identity Management Deployment"
- Section 2.7, "Locating the Required Java Development Kit (JDK)"
- Section 2.8, "Installing the Oracle Identity Management Lifecycle Tools"
- Section 2.9, "Applying Patches and Workarounds"
- Section 2.10, "Optionally Running Repository Creation Utility (RCU) to Create the Required Schemas"

2.1 Verifying Certification, System Requirements, and Interoperability

The certification matrix and system requirements documents should be used in conjunction with each other to verify that your environment meets the necessary requirements for installation.

Step 1 Verifying Your Environment Meets Certification Requirements

Make sure that you are installing your product on a supported hardware and software configuration. For more information, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

Oracle has tested and verified the performance of your product on all certified systems and environments; whenever new certifications occur, they are added to the proper certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

Step 2 Using the System Requirements Document to Verify Certification

The *Oracle Fusion Middleware System Requirements and Specifications* document should be used to verify that the requirements of the certification are met. For example, if the certification document indicates that your product is certified for installation on 64-Bit Oracle Linux 5, this document should be used to verify that your Oracle Linux 5 system has met the required minimum specifications, like disk space, available memory, specific platform packages and patches, and other operating system-specific items. System requirements can be updated at any time, and for this reason the system requirement documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

Step 3 Verifying Interoperability Among Multiple Products

The *Oracle Fusion Middleware Interoperability and Compatibility Guide for Oracle Identity and Access Management* document defines interoperability, defines compatibility, and describes how multiple Fusion Middleware products from the same release or mixed releases may be used with each other. You should read this document if you are planning to install multiple Fusion Middleware products on your system.

2.2 Running the Health Check Utility to Verify Basic System Requirements

After you review the certification and system requirements information, you can run the Oracle Identity and Access Environment Health Check Utility to automatically check your environment before you use the LCM Tools.

For more information, see the following topics:

- Section 2.2.1, "Understanding the Oracle Identity and Access Environment Health Check Utility"
- Section 2.2.2, "Running the Environment Health Check Utility Before Installing the LCM Tools"

2.2.1 Understanding the Oracle Identity and Access Environment Health Check Utility

The Oracle Identity and Access Environment Health Check Utility is a utility that you can use to verify various configurations and perform validation checks against your Oracle Identity and Access Management setup. You can run the Health Check Utility any number of times during the post-configuration stage of a manual deployment of Oracle Identity and Access Management to assist you in verifying your installation and configuration.

When you run the Health Check Utility, the utility retrieves data from your environment, uses the data to run a set of validation checks, and generates a report that provides detailed information about any issues the utility finds for each of the items it checks.

For information about the Oracle Identity and Access Environment Health Check Utility, see "Understanding the Oracle Identity and Access Environment Health Check

Utility" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.

2.2.2 Running the Environment Health Check Utility Before Installing the LCM Tools

Before you install the LCM Tools or run the Deployment Wizard, Oracle recommends that you run the Environment Health Check Utility to verify that your environment meets the minimum requirements for running the deployment wizard and creating the response file.

For this reason, you can download the Environment Health Check Utility independently of the LCM Tools, and you can run it before you have installed any Oracle Identity and Access Management or LCM software.

To perform the initial verification before running the Deployment Wizard:

1. Download the **Oracle Identity and Access Management Health Check Utility** and unpack it in a directory on your local disk.

   For more information about where to obtain the utility, see the *Oracle Identity and Access Management Download, Installation, and Configuration ReadMe* file on the Oracle Technology Network (OTN).

2. Download and install a supported Java Development Kit (JDK).

   At the time this document was published, the recommended JDK was Oracle JDK 1.7.0_55+, which can be downloaded from the Java SE Development Kit 7 Downloads page on OTN.

   For the latest information about supported configurations, see the *Oracle Fusion Middleware 11g Release 1 (11.1.1.x) Certification Matrix* on the Oracle Fusion Middleware Supported System Configurations page on OTN.

   Note that you can also get a supported JDK as part of the LCM Tools repository download. For more information, see Section 2.4 and Section Section 2.7.

3. Set the `JAVA_HOME` environment variable to the full path of your JDK directory.

4. Change directory to the following directory where downloaded and unpacked the Environment Health Check Utility:

   ```
   cd download_directory/healthcheck/bin
   ```

5. Run the following command to perform the pre-installation validation checks:

   ```
   ./idmhc.sh -manifest ../config/PreInstallChecks_mandatory_manual.xml
   ```

   Note: For more information about the pre-installation checks performed by the Environment Health Check Utility, see "PreInstallChecks_mandatory_manual.xml" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.

6. If any health checks fail, refer to the output in the Health Check Utility log files and reports to find the corrective actions. Note that the log file location will be printed on the screen after the utility is executed.

   The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful. For more information about the log files and reports, see "Analyzing Health Check Reports" in *Oracle*

Fusion Middleware Verifying Your Oracle Identity and Access Management Environment.

2.3 Understanding the Directory Server Requirements for Oracle Identity Management

For topologies that require an LDAP directory, you can either have the LCM Tools automatically create and configure a new directory instance for you, or you can manually prepare an existing LDAP directory for use with Oracle Identity Management.

For more information, see the following topics:

- Section 2.3.1, "What LDAP Directories Are Supported by Oracle Identity Management?"
- Section 2.3.2, "What Topologies Require an LDAP Directory?"
- Section 2.3.3, "How Do I Prepare an Existing LDAP Directory for Oracle Identity Management"

2.3.1 What LDAP Directories Are Supported by Oracle Identity Management?

The following directory services are supported by the LCM Tools and the Oracle Identity and Access Management software:

- If you using the LCM tools to automatically create a new directory service, you can create a new Oracle Unified Directory (OUD) or Oracle Internet Directory (OID) directory.
- If you are preparing an existing directory instance, you can use an existing OUD, OID, or Microsoft Active Directory instance.

2.3.2 What Topologies Require an LDAP Directory?

You must create a new LDAP Directory or configure an existing LDAP Directory:

- If you are deploying the Oracle Access Manager Only topology, because Oracle Access Manager requires a supported LDAP directory instance
- If you are installing both Oracle Identity Management and Oracle Access Manager and you plan to integrate the two products.

2.3.3 How Do I Prepare an Existing LDAP Directory for Oracle Identity Management

If you decide that you want to use an existing LDAP directory service that you've already installed and configured, then you must prepare the existing directory for use with Oracle Identity Management.

The procedure you use depends upon the Oracle Identity Management topology and products you are installing. Chapter 3 contains the following procedures for preparing your existing LDAP directory for Oracle Identity Management:

- Section 3.1, "Preparing an Existing OUD or OID Directory Service for Use with an Automated Oracle Identity and Access Management Deployment"
- Section 3.2, "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management"

2.4 Obtaining the LCM Tools and Oracle Identity Management Software Repository

Before you can use the LCM Tools to automate the deployment of Oracle Identity Management, you must locate and download the **Oracle Identity Management Deployment Repository**.

The repository is packaged as a set of downloadable archives. When unpacked, these archives provide you with the LCM Tools and the various software installers required to install and configure Oracle Identity and Access Management sofware.

For information about locating and downloading the repository, see the *Oracle Fusion Middleware Download, Installation, and Configuration Readme Files*.

2.5 About the Deployment Repository and LCM Tools Directory Structure

When you unpack the downloadable archives for the Oracle Identity and Access Management Deployment Repository, you create a Repository home directory. This directory is one of several key directories identified in Figure 2–1.

Table 2–1 describes each of these key directories, their purpose and how they get created.

Note that the diagram shows a recommended directory structure for a single-host deployment, where all the key directories are created on a common disk (in this example, `/u01`). In fact, you can create these directories on shared storage volumes, as long as the directories are accessible, writable, and identified in the file Locations screen of the Deployment Wizard when you are creating the response file.

For more information about using the Deployment Wizard to create the response file, see Chapter 4.

Figure 2–1 Diagram of the Complete LCM Home Directory Structure

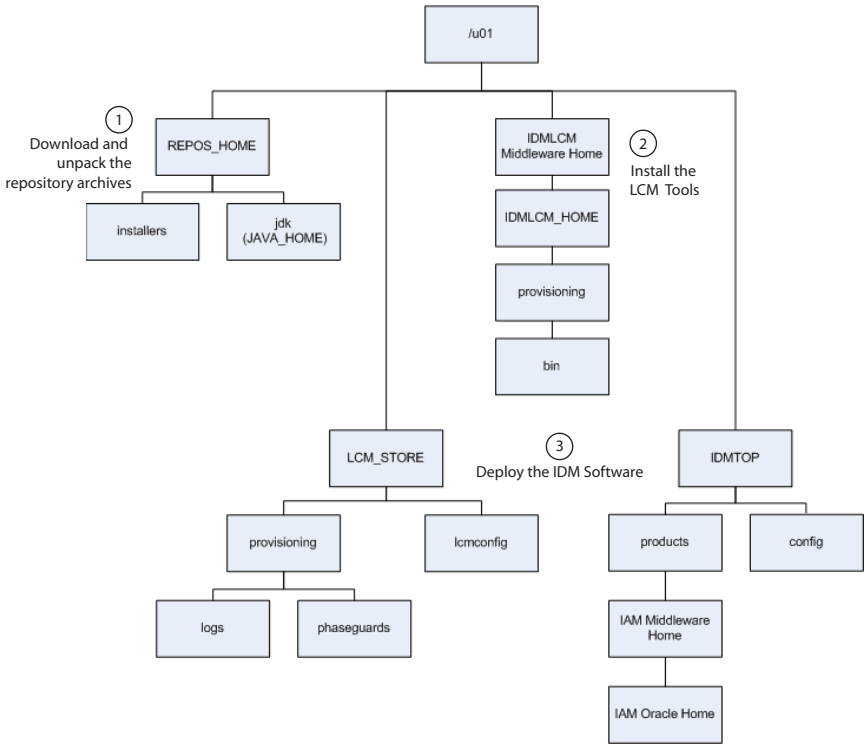


Table 2–1 Key Directories Used by the LCM Tools

Directory	Purpose	When Created	Where to Specify During Install and Deployment
REPOS_HOME	Contains the required Java Development Kit (JDK) and all the product installers required to install and configure Oracle Identity Management.	This directory is created when you unpack the Repository archives from the Oracle Technology Network (OTN).	Enter the value of the REPOS_HOME in the **Software Repository Location** field of the Deployment Wizard when you are creating a response file.
IDMLCM_HOME	Oracle home for the LCM Tools. From this directory structure, you run the LCM Deployment Wizard.	This directory is created by the LCM Tools installer.	Enter in the **Oracle Home Directory** field in the IDM LCM Tools Installer.
IDMTOP	Top-level directory for the Oracle Identity Management environment. It consists of: ■ **`IDMTOP/products`**, which contains the software binaries ■ **`IDMTOP/config`**, which contains the domains, instances, and other runtime artifacts	The IDMTOP directory, as well as its subdirectories, are created by the LCM Tools during the deployment of the Oracle Identity Management software.	In the Deployment Wizard, when creating the response file: ■ Enter the location of IDMTOP in the **Software Installation Location** field. ■ Enter the location of the `config` directory in the **Shared Configuration Location** field. **Note:** The configuration location is set to a location inside the IDMTOP directory by default; however, you can have the Deployment Wizard create the directory in any accessible location. The `products` directory will be created inside the IDMTOP directory when you deploy the software.
LCM_STORE	Contains the logs, topology.xml, and other software artifacts required by the LCM tools.	The LCM_STORE directory is created by the LCM Tools during deployment of the Oracle Identity and Access Management software.	Enter the value of the LCM_STORE variable in the **Life Cycle Management Store Location** field.

Note: It is important that minimum privileges are assigned to UNIX users in the Repository home (REPOS_HOME). In order to do this, navigate to the extracted Repository home, and run the following command. This updates the permissions on the content of the repository.

```
chmod -R 755 *
```

2.6 About Preparing a Database for an Oracle Identity Management Deployment

Before you can install and configure Oracle Identity Management, you must install and configure a supported database. The database is used to host the required schemas for each of the Oracle Identity Management components.

You can use an existing database or you can use the database installation software that is included in the downloadable LCM Tools Repository.

- To use the software available in the LCM Tools Repository, download the repository, using the instructions in Section 2.4, and then navigate to the following directory to install the database:

  REPOS_HOME/installers/database/

  For information about locating the REPOS_HOME directory, see Section 2.5.

- If you want to use an existing database, see the section "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications* to be sure your database meets the minimum system requirements for the LCM Tools and the Oracle Identity and Access Management software.

Note that starting with Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3), you can optionally install the schemas in the database, using the LCM Tools. This means you no longer have to install the schemas manually using the Repository Creation Utility.

2.7 Locating the Required Java Development Kit (JDK)

After you expand the archives and create the Repository home (REPOS_HOME), you can find an expanded copy of the supported Java Development (JDK) in the following directory:

REPOS_HOME/jdk

Before you start the LCM Tools installer, set the JAVA_HOME system variable to point to this directory.

2.8 Installing the Oracle Identity Management Lifecycle Tools

The Oracle Identity Management Deployment Wizard is a component of the Oracle Identity Management Lifecycle Tools, which also includes the Oracle Identity Management Patching Framework. You must install the tools by running an installer, which is located in the Oracle Identity Management deployment repository.

For more information, see the following topics:

- Section 2.8.1, "Locating and Starting the LCM Tools Installer"
- Section 2.8.2, "Summary of the LCM Tools Installer Screens"
- Section 2.8.3, "Specifying an Inventory Directory"

2.8.1 Locating and Starting the LCM Tools Installer

The installation script for the Oracle Identity Management Lifecycle Tools (IAM Deployment Wizard and IAM Patching Tools) resides in the following directory:

REPOS_HOME/installers/idmlcm/Disk1

where *REPOS_HOME* is the Oracle Identity Management deployment repository that contains all the installers required to deploy a new Oracle Identity Management environment.

To begin installing the tools, change to that directory and start the script.

On UNIX:

```
cd REPOS_HOME/installers/idmlcm/Disk1
./runInstaller -jreLoc <full path to the JRE directory>
```

For example:

```
./runInstaller -jreLoc REPOS_HOME/jdk
```

2.8.2 Summary of the LCM Tools Installer Screens

Table 2–2 describes each of the LCM Tools installer screens.

Table 2–2 Installation Flow for Identity Management LCM Tools

Screen	Description and Action Required
Welcome	Review the information on the Welcome page, and click **Next**.
Specify Inventory Directory	This screen appears if this is the first time you are installing Oracle software on a UNIX host or if you installed software previously on the UNIX host, but did not create a central inventory. The Inventory Directory is used to keep track of all Oracle products installed on this host. For the purposes of this guide: 1. Click **OK** to accept the default location of the Inventory Directory and the default Operating System Group Name for the directory. 2. In the Inventory Location Confirmation dialog box, select **Continue Installation with local inventory**. If you want to create a central Inventory Directory or learn about the advantages of doing so, see Section 2.8.3.
Prerequisite Checks	On this screen, verify that checks complete successfully, then click **Next**.

Specify Install Location	On the Specify Install Location page, enter the following information:
	1. **Oracle Middleware Home** - This is the parent directory of the directory where the Identity and Access Management Lifecycle Tools will be installed. For example:
	`/u01/Oracle/Middleware/`
	2. **Oracle Home Directory** - The Oracle home a subdirectory of the Oracle Middleware Home for the LCM Tools.
	`/u01/Oracle/Middleware/idmlcm/`
	In the this guide, this subdirectory is referred to as the Identity and Access Management Life Cycle Management Oracle home (IDMLCM_HOME.)
	Click **Next**.

Installation Summary	Verify the information on this screen, then click **Install** to begin the installation.
Installation Progress	This screen shows the progress of the installation. When the progress shows 100% complete, click **Next** to continue
Installation Complete	On the Installation Complete page, click **Finish**.

2.8.3 Specifying an Inventory Directory

If you are running on a UNIX platform, and you have not previously installed an Oracle product on this host, or if you installed software previously on the UNIX host,

but did not create a central inventory, then the Specify Inventory Directory screen will appear during the installation.

The Specify Inventory Directory screen prompts you for the location of the **Inventory Directory**. The Inventory Directory is used to keep track of all Oracle products installed on this host.

You can save a local inventory directory just for the software you are currently installing, or you can create a central inventory directory for all Oracle software installed on the host, even software installed by other users.

A central inventory directory can be especially important when you are performing life cycle operations, such as patching, test-to-production, or when upgrading your software to a newer version.

To create a central inventory directory:

1. In the **Operating System Group ID** field, select the group whose members you want to grant access to the inventory directory.

   All members of this group can install products on this host and write to the inventory directory.

   Click **OK** to continue.

2. The **Inventory Location Confirmation** dialog prompts you to run the *inventory_directory*`/createCentralInventory.sh` script as `root` to create the `/etc/oraInst.loc` file.

   The /etc/oraInst.loc file is a pointer to the central inventory and must be present for silent installations. It contains two lines:

   `inventory_loc=`*`path_to_central_inventory`*

   `inst_group=`*`install_group`*

   The standard location for this file is `/etc/oraInst.loc`, but it can be created anywhere. If you create it in a directory other than `/etc`, you must include the `-invPtrLoc` argument and enter the location of the inventory when you run the `Identity and Access Management Deployment Wizard` or the `runIAMDeployment.sh` script.

2.9 Applying Patches and Workarounds

The LCM Tools Repository will sometimes include patches that will be applied automatically during the automatic deployment of Oracle Identity and Access Management.

In addition, there might be cases where additional patches are required to address specific known issues. See the section "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Identity Management Release Notes* for a list of patches to apply. You **must** apply the patches to ensure that your software operates as expected.

Before starting the deployment, download any patches that are listed in the Release Notes, plus any other patches that are appropriate for your environment. Unzip each patch to the directory appropriate for the product, as listed in Table 2–3. If the directory does not exist, create it.

Patches are available for download from `http://support.oracle.com`. You can find instructions for deploying each patch in the enclosed `README.html` file.

After unzipping the patch, make sure that the Patch Directory (as listed in Table 2–3) contains a directory which is a number. That directory contains directories and files similar to:

- etc
- files
- README.txt

This is the directory layout for most patches. In some cases, such as bundle patches, the layout might be similar to:

bundle_patch_no/*product*/*product_patch_no*

In this case make sure that it is *product_patch_no* which appears in the Patch Directory not *bundle_patch_no*.

If a bundle patch contains fixes for multiple products make sure that the individual patches appear in the correct Patch Directory as listed below.

Table 2–3 Product Patch Directories

Product	Patch Directory
Oracle Access Management Access Manager	*REPOS_HOME*/installers/iamsuite/patch/oam
Oracle HTTP Server	*REPOS_HOME*/installers/webtier/patch
WebGate	*REPOS_HOME*/installers/webgate/patch
Oracle Identity Manager	*REPOS_HOME*/installers/iamsuite/patch/oim
SOA Suite	*REPOS_HOME*/installers/soa/patch
WebLogic Server	*REPOS_HOME*/installers/smart_update/weblogic
suwrapper	*REPOS_HOME*/installers/smart_update/suwrapper
Oracle Unified Directory	*REPOS_HOME*/installers/oud/patch
Oracle Internet Directory	*REPOS_HOME*/installers/idm/patch/oid
Business Intelligence Publisher (BIP)	*REPOS_HOME*/installers/iamsuite/patch/bip
Mobile Security Manager	*REPOS_HOME*/installers/iamsuite/patch/msm
Mobile Security Access Server	*REPOS_HOME*/installers/omsas/patch

2.9.1 Mandatory Patches Required for Installing Oracle Identity Manager

There are some mandatory patches that must be applied for installing and configuring Oracle Identity Manager. For more information about these patches, see the section Mandatory Patches Required for Installing Oracle Identity Manager in the *Oracle Fusion Middleware Identity Management Release Notes*.

In addition, Oracle Identity Manager also requires specific database patches. For more information, see the section Patch Requirements in the *Oracle Fusion Middleware Identity Management Release Notes*.

2.10 Optionally Running Repository Creation Utility (RCU) to Create the Required Schemas

Starting with Oracle Identity Management 11g Release 2 (11.1.2.3), you can use the LCM Tools to install the required schemas as part of the deployment process.

Optionally, you can choose to use the Oracle Identity Management version of RCU to install the schemas before you install and run the LCM Tools.

> **Important:** If you choose to run RCU yourself, then be sure to use the version provided in the LCM Tools Repository; otherwise, the Oracle Identity and Access Management configuration might fail.

For more information, see the following:

- Section 2.10.1, "Locating and Starting RCU to Prepare for an Automated Deployment"
- Section 2.10.2, "Using RCU to Install the Required Oracle Identity Management Schemas"

2.10.1 Locating and Starting RCU to Prepare for an Automated Deployment

If you choose to install the schemas manually using RCU, then you can locate the RCU software in the following directory:

REPOS_HOME/installers/fmw_rcu/linux/rcuHome.zip

In this path, *REPOS_HOME* is the Oracle Identity Management deployment repository that contains all the installers required to deploy a new Oracle Identity Management environment.

Extract the contents of the rcuHome.zip file to a directory of your choice; this directory is referred to as the *RCU_HOME* directory.

Start the RCU from the bin directory inside the *RCU_HOME* directory.

On UNIX:

```
cd RCU_HOME/bin
```

```
./rcu
```

2.10.2 Using RCU to Install the Required Oracle Identity Management Schemas

The options you select when running RCU will vary, depending upon the topology you want to deploy. For more information about the topologies supported by the :LCM Tools, see Section 1.4, "Understanding the Supported Oracle Identity Manager Topologies".

After you start RCU, use the instructions in "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*, and refer to the following topics:

- Section 2.10.2.1, "Considerations When Using RCU to Install the Schemas for an Automated Deployment"
- Section 2.10.2.2, "Selecting the Required Schemas for Supported Automated Installation Topologies"

2.10.2.1 Considerations When Using RCU to Install the Schemas for an Automated Deployment

As you navigate through the RCU screens and select the required schemas, note the following important considerations:

- Installing required schemas as part of deployment process is supported only on Linux platforms.

  This is because underlying RCU support is only available on Linux and not on other unix platforms. Customers from other platforms like Solaris, AIX and HP Itanium need to install required schemas manuallly using Oracle Identity and Access Management version of RCU.

- Be sure to select one password for all schemas you install.

  This is a requirement of the LCM Tools automated installation.

- If you are deploying an integrated, OIM, OAM, and OMSS environment, then you can use either separate, dedicated databases for OIM and OAM or a single consolidated database.

  If you are using a consolidated database, then you must different prefixes for the OAM and OIM schemas, and you must create two separate OPSS schemas, one for each domain. This will allow you to upgrade the OIM or OAM separately at a later time.

- Be sure to remember the schema prefix, host, port, servicename, username, and password that you provide when creating the schemas using RCU. You will need to provide this information when you create the deployment response in Chapter 4, "Creating a Deployment Response File".

2.10.2.2 Selecting the Required Schemas for Supported Automated Installation Topologies

When you run RCU, create and load only the following schemas for the Oracle Identity and Access Management component you are installing—do not select any other schemas available in RCU:

- If you are deploying the Oracle Identity Manager (OIM) Only topology, then select the **Identity Management - Oracle Identity Manager** schema.

  When you select the **Identity Management - Oracle Identity Manager** schema, the following schemas are also selected, by default:

  - **SOA and BPM Infrastructure - SOA Infrastructure**
  - **SOA and BPM Infrastructure - User Messaging Service**
  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**
  - **Oracle Business Intelligence - Business Intelligence Platform**

- If you are deploying the Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS) Only topology, then select the **Identity Management - Oracle Mobile Security Manager** schema.

  By default, Oracle Mobile Security Suite is installed (but not fully configured) with Oracle Access Management. You can choose to configure Oracle Access Management only or configure Oracle Access Management with Oracle Mobile Security Suite. For both configuration options, you must select the **Identity Management - Oracle Mobile Security Manager** schema.

When you select the **Identity Management - Oracle Mobile Security Manager** schema, the following schemas are also selected, by default:

- **AS Common Schemas - Oracle Platform Security Services**
- **AS Common Schemas - Metadata Services**
- **AS Common Schemas - Audit Services**
- **Identity Management - Oracle Access Manager**

- If you are deploying the OIM-OAM-OMSS Integrated with Directory topology, then you must run RCU twice, once to install the schemas required for OIM and once to install the schemas required for Oracle Access Manager and Oracle Mobile Security Services.

  Be sure to use a different schema prefix each time you run RCU. For more information, see Section 2.10.2.1.

3

Preparing an Existing Directory Service for Oracle Identity and Access Management

Use this chapter to prepare an existing and supported LDAP directory for use with Oracle Identity and Access Management.

For information about when you need to perform the procedures in this chapter, see Section 2.3, "Understanding the Directory Server Requirements for Oracle Identity Management".

This chapter contains the following sections:

- Section 3.1, "Preparing an Existing OUD or OID Directory Service for Use with an Automated Oracle Identity and Access Management Deployment"
- Section 3.2, "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management"
- Section 3.3, "Configuring Active Directory in SSL Mode"

3.1 Preparing an Existing OUD or OID Directory Service for Use with an Automated Oracle Identity and Access Management Deployment

To set up the directory instances for OUD and OID, perform the following tasks:

- Section 3.1.1, "About the idmConfigTool_STA Script"
- Section 3.1.2, "Setting up Environment Variables to Run the idmConfigTool_STA Script"
- Section 3.1.3, "Editing the Properties File for the idmConfigTool_STA Script"
- Section 3.1.4, "Preparing a Password File"
- Section 3.1.5, "Running the preConfigIDStore Command"
- Section 3.1.6, "Running the prepareIDStore Command"
- Section 3.1.7, "Ensuring the Success of Running idmConfigTool"

3.1.1 About the idmConfigTool_STA Script

Before you can use an existing directory service as part of an Oracle Identity and Access Management deployment, you must prepare the directory by adding the required users, groups, containers and other required artifacts.

To perform this task, you use a special, standalone version the `idmConfigTool` script, which is packaged as part of the LCM Tools.

The standalone version of the idmConfigTool_STA script is called idmConfigTool_STA, and it is installed in the following location in the LCM Tools Oracle home (IDMLCM_HOME) when you install the LCM Tools:

IDMLCM_HOME/existing_directory/idmtools/bin

For more information about locating this directory and the idmConfigTool_STA script, see the following:

- Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure"
- Section 2.8, "Installing the Oracle Identity Management Lifecycle Tools"

3.1.2 Setting up Environment Variables to Run the idmConfigTool_STA Script

Before you can run the idmConfigTool_STA script, you must set the following operating system environment variables. Set these variables in the same terminal window you will use to run the idmConfigTool_STA script:

- ORACLE_HOME

  Set this variable to the following directory:

  IDMLCM_HOME/existing_directory

  In this example, replace *IDMLCM_HOME* with the value of the IDMLCM_HOME variable in Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

  Note that for most LCM Tools operations, the Oracle home is typically considered the value of IDMLCM_HOME, but to run the idmConfigTool_STA script, you must set this value to the existing_directory subdirectory inside IDMLCM_HOME.

- JAVA_HOME

  The complete path to a supported Java Development Kit (JDK). Note that JDK can be obtained from repository shipped for IDMLCM.

3.1.3 Editing the Properties File for the idmConfigTool_STA Script

The LCM Tools provide a properties file that you use to provide input to the idmConfigTool_STA script. The file is installed the following location inside the LCM Oracle home:

IDMLCM_HOME/existing_directory/idmtools/input_parameters.properties

Open the input_parameters.properties file with a text editor and follow the instructions in the file.

For each parameter, provide a value, so the idmConfigTool_STA script can locate and connect to the directory service and then make the required changes to the directory.

Note that the input_parameters.properties file contains two specific sections:

- The preConfigIDStore properties
- The prepareIDStore properties

Many of the properties in the preConfigIDStore section of the file have default values, but be sure to review all the values, because some of the properties, such as the host name, must be modified. For others, you can take the default values if they apply.

Most of the values in the prepareIDStore section of the file can be left as is. They represent standard values for Directory Service data required by each of the Oracle Identity and Access Management components. For example, the default values expected for Oracle Access Manager are shown in the section marked #OAM.

3.1.4 Preparing a Password File

The idmConfigTool_STA script requires passwords to connect to the LDAP directory and to connect to the WebLogic Administration Server. It also requires you to create new passwords for the system and administrative accounts that it creates in the LDAP directory.

You can provide these passwords in one of two ways:

- You can interactively provide the passwords when prompted by idmConfigTool_STA script.

  OR

- You can create a password file that is provided an input file to the idmConfigTool_STA script.

If you decide to create a password file, you can then run the idmConfigTool script without human interaction.

To create a password file:

1. Use a text editor to create a text file.

   You can use any file name or location, as long as it is accessible to the idmConfigTool_STA script.

2. Enter the following password values in the file:

```
IDSTORE_PASSWD: your_value
IDSTORE_PWD_READONLYUSER: your_value
IDSTORE_PWD_READWRITEUSER: your_value
IDSTORE_PWD_SUPERUSER: your_value
IDSTORE_PWD_OAMSOFTWAREUSER: your_value
IDSTORE_PWD_OAMADMINUSER: your_value
IDSTORE_PWD_OAMOBLIXUSER: your_value
IDSTORE_PWD_OIMADMINUSER: your_value
IDSTORE_ADMIN_PASSWD: your_value
WLSPASSWD: your_value
IDSTORE_PWD_XELSYSADMINUSER: your_value
IDSTORE_PWD_WEBLOGICADMINUSER: your_value
```

Note that the values you enter in this password file will be encrypted for security purposes when you run idmConfigTool_STA script.

3.1.5 Running the preConfigIDStore Command

Running the preConfigIDStore command seeds the required objectclasses into LDAP directory.

Run the following command to perform this task:

1. Change directory to the following location in the IDM LCM Tools Oracle home:

```
cd IDMLCM_HOME/existing_directory/idmtools/bin/
```

2. Run the idmConfigTool_STA script as follows:

```
./idmConfigTool_STA.sh -preConfigIDStore \
```

```
input_file=input_parameters.properties \
pwd_file=password_input_file \
log_file=log_file_name
```

Note: In this example, be sure to provide a name and location for the log file that will be created by the `idmConfigTool_STA` script. The script does not provide any errors when it is run. The only way to verify the successful completion of the script is by reviewing the log file and searching for SEVERE log entries.

3.1.6 Running the prepareIDStore Command

Running the `prepareIDStore` command creates the required users, groups, containers, and other required artifacts in LDAP directory.

Run the following commands to perform this task:

1. Change directory to the following location in the IDM LCM Tools Oracle home:

   ```
   cd IDMLCM_HOME/existing_directory/idmtools/bin
   ```

2. Run the `idmConfigTool_STA` script once for each of the primary components, Oracle WebLogic Server, Oracle Access Manager, and Oracle Identity Manager, as applicable to your specific topology.

   You must always run the script for Oracle WebLogic Server (WLS), but run the Oracle Access Manager (OAM) and Oracle Identity Manager commands only if they apply to your topology:

   ```
   ./idmConfigTool_STA.sh -prepareIDStore \
         mode=WLS \
         input_file=input_parameters.properties \
         pwd_file=password_input_file \
         log_file=log file

   ./idmConfigTool_STA.sh -prepareIDStore \
         mode=OAM \
         input_file=input_parameters.properties \
         pwd_file=password_input_file \
         log_file=log file

   ./idmConfigTool_STA.sh -prepareIDStore \
         mode=OIM \
         input_file=input_parameters.properties \
         pwd_file=password_input_file \
         log_file=log_file
   ```

   In this example, be sure to provide a name and location for the log file that will be created by the `idmConfigTool` script. The script does not provide any errors when it is run. The only way to verify the successful completion of the script is by reviewing the log file.

3.1.7 Ensuring the Success of Running idmConfigTool

The `idmConfigTool` does not display errors or provide return code. The only way to ensure that the operation is completed successfully is to ensure that there are no **SEVERE** tags in the logs generated.

The location of the log file is determined by the value you assigned to the `log_file` argument on the `idmConfigTool_STA` command line. For more information, see Section 3.1.5 and Section 3.1.6.

3.2 Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management

To set up the directory instance of Active Directory, perform the following tasks:

- Section 3.2.1, "Adding the Required Schemas to the Active Directory Instance"
- Section 3.2.2, "Creating the Required Containers in the Active Directory Instance"
- Section 3.2.3, "Adding Access Control Lists (ACLs) to the Containers in Active Directory"
- Section 3.2.4, "Creating Users in the Active Directory Instance"
- Section 3.2.5, "Adding User Memberships to Groups in an Active Directory Instance"
- Section 3.2.6, "Assigning Administrator Privileges to the OIMAdministrators Group"
- Section 3.2.7, "Resetting User Passwords in an Active Directory Instance"
- Section 3.2.8, "Enabling User Accounts for in an Active Directory Instance"
- Section 3.2.9, "Setting the LockoutThreshold in Active Directory"

About Enabling SSL for Active Directory: If you are deploying an OAM and OMSS topology, then you can optionally enable SSL for the Active Directory, using the additional setup instructions in Section 3.3.

If you are deploying an integrated OIM, OAM, and OMSS topology, then you must enable SSL for the Active Directory, using the additoinal setup instructions in Section 3.3.

3.2.1 Adding the Required Schemas to the Active Directory Instance

The first step in preparing an existing Active Directory instance for an automatic deployment with the LCM Tools is to load the required schemas into the directory.

Oracle provides the schemas as a set of LDIF files that you can edit and then import into the Active Directory instance.

To load the schemas into the existing Active Directory instance:

1. Change directory to the following directory:in the LCM Tools home directory (IDMLCM_HOME):

   IDMLCM_HOME`/existing_directories/idmtools/templates/ad/`

Note: If you are deploying Oracle Identity and Access Management manually, without the LCM Tools, then the schema LDIF files can be found in the following directory in the Oracle Identity and Access Management Oracle home after you install the software:

IAM_ORACLE_HOME`/oam/server/oim-intg/ldif/ad/schema/`

---

2. Open the LDIF files required for your topology with a text editor and replace all occurrences of `<domain-dn>` with the distinguished name (DN) for your organization:

   - If you are planning to deploy an OAM and OMSS topology, then edit the following LDIF files:

     ```
     AD_OracleSchema.ldif
     AD_OblixSchema.ldif
     ```

     Note: If you are planning to use OMSS and Active Directory without the OAM password management functionality, then it is not mandatory to use the `AD_OracleSchema` and `AD_OblixSchema` LDIF files to extend the Active Directory schema.

   - If you are planning to deploy an integrated OIM, OAM, and OMSS topology, then edit the following LDIF files:

     ```
     AD_OracleSchema.ldif
     AD_UserSchema.ldif
     AD_oam_pwd_schema_add.ldif
     ```

3. Use your standard procedures to import the applicable LDIF files into the Active Directory instance.

   For more information about loading an LDIF file, refer to the Active Directory documentation.

3.2.2 Creating the Required Containers in the Active Directory Instance

After you install the required schemas in an existing Active Directory instance, you can then create the required containers within the directory instance.

To create the required containers:

1. Create a new LDIF file that can be used to create the containers required for your topology.

   - If you are planning to deploy an OAM and OMSS topology, then create an .ldif file as shown in Example 3–1.
   - If you are planning to deploy an integrated OIM, OAM, and OMSS topology, then create an .ldif file as shown in Example 3–2.

   Note that both sample .ldif files use the following as a placeholder for the actual domain container for your organization. Be sure to replace the following with the information applicable to your environment:

   ```
   dc=example,dc=com
   ```

2. Use your standard procedures to import the LDIF file into the Active Directory instance.

Example 3–1 Sample LDIF File Used to Create Containers for an OAM and OMSS Deployment

```
dn: cn=Groups,dc=example,dc=com
changetype: add
cn: Groups
objectclass: container
```

```
dn: cn=SystemIDs,dc=example,dc=com
changetype: add
cn: SystemIDs
objectclass: container

dn: cn=orclFAUserReadPrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAUserReadPrivilegeGroup
objectclass: group

dn: cn=orclFAUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAUserWritePrivilegeGroup
objectclass: group

dn: cn=orclFAUserWritePrefsPrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAUserWritePrefsPrivilegeGroup
objectclass: group

dn: cn=orclFAGroupReadPrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAGroupReadPrivilegeGroup
objectclass: group

dn: cn=orclFAGroupWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAGroupWritePrivilegeGroup
objectclass: group

dn: cn=orclFAOAMUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAOAMUserWritePrivilegeGroup
objectclass: group

dn: cn=IDM Administrators,cn=Groups,dc=example,dc=com
changetype: add
cn: IDM Administrators
objectclass: group

dn: cn=OAMAdministrators,cn=Groups,dc=example,dc=com
changetype: add
cn: OAMAdministrators
objectclass: group
```

Example 3–2 Sample LDIF File to Create Containers for an Integrated OIM, OAM, and OMSS Topology

```
dn: cn=Groups,dc=example,dc=com
changetype: add
cn: Groups
objectclass: container

dn: cn=SystemIDs,dc=example,dc=com
changetype: add
cn: SystemIDs
objectclass: container

dn: cn=reserve,cn=Groups,dc=example,dc=com
changetype: add
```

```
cn: reserve
objectclass: container

dn: cn=orclFAUserReadPrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAUserReadPrivilegeGroup
objectclass: group

dn: cn=orclFAUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAUserWritePrivilegeGroup
objectclass: group

dn: cn=orclFAGroupReadPrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAGroupReadPrivilegeGroup
objectclass: group

dn: cn=orclFAGroupWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAGroupWritePrivilegeGroup
objectclass: group

dn: cn=orclFAOAMUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
changetype: add
cn: orclFAOAMUserWritePrivilegeGroup
objectclass: group

dn: cn=IDM Administrators,cn=Groups,dc=example,dc=com
changetype: add
cn: IDM Administrators
sAMAccountName: IDM Administrators
objectclass: group

dn: cn=OAMAdministrators,cn=Groups,dc=example,dc=com
changetype: add
cn: OAMAdministrators
sAMAccountName: OAMAdministrators
objectclass: group

dn: cn=OIMAdministrators,cn=Groups,dc=example,dc=com
changetype: add
cn: OIMAdministrators
sAMAccountName: OIMAdministrators
objectclass: group

dn: cn=BIReportAdministrator,cn=Groups,dc=example,dc=com
changetype: add
cn: BIReportAdministrator
sAMAccountName: BIReportAdministrator
objectclass: group
```

3.2.3 Adding Access Control Lists (ACLs) to the Containers in Active Directory

After you create the required containers in the Active Directory instance, you can then set the privileges for each container, using Access Control Lists (ACLs).

Follow the instructions in the following article on the Microsoft TechNet Web site to add the ACLs listed in Example 3–3:

`http://technet.microsoft.com/en-us/library/cc757520%28v=ws.10%29.aspx`

Example 3–3 List of ACLs for the Required Active Directory Containers

```
orclFAUserReadPrivilegeGroup : Read privileges to users container
orclFAUserWritePrivilegeGroup : Write privileges to users container
orclFAGroupReadPrivilegeGroup : Read privileges to groups container
orclFAGroupWritePrivilegeGroup : Write privileges to groups container
orclFAOAMUserWritePrivilegeGroup : Write privileges to users and groups container
```

3.2.4 Creating Users in the Active Directory Instance

After you have created the containers within the Active Directory instance, then you can create the required users:

1. Create a new LDIF file that can be used to create the users required for your topology:
   - If you are planning to deploy an OAM and OMSS topology, then create an .ldif file as shown in Example 3–4.
   - If you are planning to deploy an integrated OIM, OAM, and OMSS topology, then create an .ldif file as shown in Example 3–5.

   Note that both sample .ldif files use the following as a placeholder for the actual domain container for your organization. Be sure to replace the following with the information applicable to your environment:

   ```
   dc=example,dc=com
   @example.com
   ```

2. Use your standard procedures to import the LDIF file into the Active Directory instance.

Example 3–4 Sample LDIF File for Adding Users to the Active Directory Instance for an OAM and OMSS Topology

```
dn: cn=weblogic_idm,cn=Users,cd=example,dc=com
changetype: add
cn: weblogic_idm
objectClass: user
samAccountName: weblogic_idm
givenName: weblogic_idm
sn: weblogic_idm
userPrincipalName: weblogic_idm@example.com

dn: cn=oamadmin,cn=Users,cd=example,dc=com
changetype: add
cn: oamadmin
objectClass: user
samAccountName: oamadmin
givenName: oamadmin
sn: oamadmin
userPrincipalName: oamadmin@example.com

dn: cn=OblixAnonymous,cd=example,dc=com
changetype: add
cn: OblixAnonymous
objectClass: user
samAccountName: OblixAnonymous
givenName: OblixAnonymous
sn: OblixAnonymous
userPrincipalName: oblixanonymous@example.com
```

```
dn: cn=oamLDAP,cn=systemids,cd=example,dc=com
changetype: add
cn: oamLDAP
objectClass: user
samAccountName: oamLDAP
givenName: oamLDAP
sn: oamLDAP
userPrincipalName: oamldap@example.com
```

Example 3–5 Sample LDIF File to Create Users in an Active Directory Instance for an Integrated OIM, OAM, and OMSS Topology

```
dn: cn=weblogic_idm,cn=Users,dc=example,dc=com
changetype: add
objectClass: user
samAccountName: weblogic_idm
givenName: weblogic_idm
sn: weblogic_idm
cn: weblogic_idm
userPrincipalName: weblogic_idm@example.com

dn: cn=xelsysadm,cn=Users,dc=example,dc=com
changetype: add
objectClass: user
samAccountName: xelsysadm
givenName: xelsysadm
sn: xelsysadm
cn: xelsysadm
userPrincipalName: xelsysadm

dn: cn=oamadmin,cn=Users,dc=example,dc=com
changetype: add
objectClass: user
samAccountName: oamadmin
givenName: oamadmin
sn: oamadmin
cn: oamadmin
userPrincipalName: oamadmin@example.com

dn: cn=OblixAnonymous,dc=example,dc=com
changetype: add
objectClass: user
samAccountName: OblixAnonymous
givenName: OblixAnonymous
sn: OblixAnonymous
cn: OblixAnonymous
userPrincipalName: oblixanonymous@example.com

dn: cn=oamLDAP,cn=systemids,dc=example,dc=com
changetype: add
objectClass: user
samAccountName: oamLDAP
givenName: oamLDAP
sn: oamLDAP
cn: oamLDAP
userPrincipalName: oamLDAP@example.com

dn: cn=oimLDAP,cn=systemids,dc=example,dc=com
changetype: add
objectClass: user
```

```
samAccountName: oimLDAP
givenName: oimLDAP
sn: oimLDAP
cn: oimLDAP
userPrincipalName: oimLDAP@example.com
```

3.2.5 Adding User Memberships to Groups in an Active Directory Instance

After you have created the users in the Active Directory instance, add each user to the appropriate group:

- For an OAM and OMSS topology, the groups and their associated users are shown in Section 3.2.5.1.
- For an integrated OIM, OAM, and OMSS deployment, the groups and their associated users are shown in Section 3.2.5.2.

For instructions on adding users to groups, see the following article on the Microsoft TechNet Web site:

`https://technet.microsoft.com/en-us/library/cc737130%28v=ws.10%29.aspx`

3.2.5.1 Summary of the Groups and Users for an OAM and OMSS Deployment

For an OAM and OMSS deployment, use the following list to assign the required users to each group:

- `cn=IDM Administrators,cn=Groups,dc=example,dc=com`
  - `cn=oamadministrators,cn=groups,dc=example,dc=com`
  - `cn=weblogic_idm,cn=users,dc=example,dc=com`
- `cn=OAMAdministrators,cn=Groups,dc=example,dc=com`
  - `cn=oamadmin,cn=users,dc=example,dc=com`
- `cn=orclFAGroupReadPrivilegeGroup,cn=Groups,dc=example,dc=com`
  - `cn=oamldap,cn=systemids,dc=example,dc=com`
- `cn=orclFAOAMUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com`
  - `cn=oamldap,cn=systemids,dc=example,dc=com`
- `cn=orclFAUserReadPrivilegeGroup,cn=Groups,dc=example,dc=com`
  - `cn=oamldap,cn=systemids,dc=example,dc=com`

3.2.5.2 Summary of the Groups and Users for an Integrated OIM, OAM, and OMSS Deployment

For an integrated OIM, OAM, and OMSS topology, use the following list to assign the required users to each group:

- `cn=IDM Administrators,cn=Groups,dc=example,dc=com`
  - `cn=oamadministrators,cn=groups,dc=example,dc=com`
  - `cn=weblogic_idm,cn=users,dc=example,dc=com`
- `cn=OAMAdministrators,cn=Groups,dc=example,dc=com`
  - `cn=oamadmin,cn=users,dc=example,dc=com`
- `cn=OIMAdministrators,cn=Groups,dc=example,dc=com`
  - `cn=oimldap,cn=systemids,dc=example,dc=com`

- cn=orclFAGroupReadPrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=orclFAOAMUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=orclFAUserReadPrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=BIReportAdministrator,cn=Groups,dc=example,dc=com
  - cn=xelsysadm,cn=Users,dc=example,dc=com

3.2.6 Assigning Administrator Privileges to the OIMAdministrators Group

For integrated OIM, OAM, and OMSS deployments, add the `OIMAdministors` group to the Administrators group, as follows:

1. In Active Directory Users and Computers, right-click the **OIMAdministrators** group.
2. Select **Properties** from the context menu.
3. Select the **Member Of** tab.
4. Click **Add** and use the Select Groups dialog box to add **Administrators**.
5. Click **OK** to close the Select Groups dialog box.
6. Click **Apply** to apply your changes.

3.2.7 Resetting User Passwords in an Active Directory Instance

After you have created the required users and assigned them to the appropriate groups, you should reset the user passwords.

To reset the user passwords, see the following article on the Microsoft TechNet Web site:

`http://technet.microsoft.com/en-in/library/cc782255%28v=ws.10%29.aspx`

Note that when you reset the password for each of the required Oracle Identity and Access Management users in the directory, clear the **User must change password at next logon** check box.

3.2.8 Enabling User Accounts for in an Active Directory Instance

After you have created the containers, set the ACLs, added the users, assigned t hem to the proper groups, and reset the user passwords, you can then enable the user accounts:

1. From the **Start** menu, select **Administrative Tools**, and then **Active Directory Users and Computers**.
2. Click each container that contains the users you have created.
3. From the Details pane, right-click each user and select **Enable Account**.

3.2.9 Setting the LockoutThreshold in Active Directory

To ensure the proper behavior when a user enters the wrong password multiple times, it important that you configure the `LockoutThreshold` value for Active Directory to match the security settings for Oracle Identity and Access Management software.

In most cases, it is best to set the the Active Directory `LockoutThreshold` to 10. However, after you deploy Oracle Identity and Access Management, you should check to see if the `pwdMaxFailure` setting in the following Oracle Identity and Access Management configuration file is also set to 10:

DOMAIN_HOME`/config/fmwconfig/ovd/oim/adapters.os_xml`

In general, you should set the Active Directory `LockoutThreshold` to match the `pwdMaxFailure` setting.

For more information about the `LockoutThreshold` setting, see the following article on the Microsoft Technet Web site:

`https://technet.microsoft.com/en-us/library/cc775412%28v=ws.10%29.aspx`

3.3 Configuring Active Directory in SSL Mode

If you are deploying an OAM and OMSS environment, configuring Active Directory in SSL Mode is an optional step.

However, If you are deploying an integrated OIM, OAM, and OMSS environment, then you must configure the Active Directory instance in SSL Mode.

1. Use the Active Directory documentation to configure the directory instance in SSL Mode.
2. Make a note of the RootCA certificate that you generate while configuring Active Directory in SSL-mode.

   This certificate will be required as an input when you are deploying the software using the LCM Tools.

Part II

Deploying Oracle Identity and Access Management

Part II provides information on creating a deployment response file. It also describes the procedure for deploying Oracle Identity and Access Management.

Part II contains the following chapters:

- Chapter 4, "Creating a Deployment Response File"
- Chapter 5, "Performing Oracle Identity and Access Management Deployment"

4

Creating a Deployment Response File

This chapter describes how to create a deployment response file using the Oracle Identity and Access Management Deployment Wizard.

This chapter contains the following sections:

- Section 4.1, "What is a Deployment Response File?"
- Section 4.2, "Starting the Deployment Wizard and Navigating the Common Screens"
- Section 4.3, "Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology"
- Section 4.4, "Creating a Deployment Response File for an Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Topology"
- Section 4.5, "Creating a Deployment Response File for an Integrated OIM, OAM, and OMSS Topology"
- Section 4.6, "Additional Information When Creating a Response File for an Automated Deployment"

4.1 What is a Deployment Response File?

Before you can perform deployment, you must provide information about your topology to the Oracle Identity and Access Management Deployment Wizard.

The Wizard collects all the information required to perform an Oracle Identity and Access Management deployment, such as ports, directory locations, and database schema.

Using this information, the wizard creates a deployment response file that you can later use to perform the actual deployment operation.

The default name of the deployment response file is `provisioning.rsp`. You can change the deployment response file name in the **Summary** screen of the Oracle Identity and Access Management Deployment Wizard.

4.2 Starting the Deployment Wizard and Navigating the Common Screens

1. Make sure you have installed a valid and supported Java Development Kit (JDK) and that you have set the JAVA_HOME environment variable.

   For more information, see Section 2.7, "Locating the Required Java Development Kit (JDK)".

2. Start the Deployment Wizard:

a. Change directory to the following directory:

```
IDMLCM_HOME/provisioning/bin
```

In this example, *IDMLCM_HOME* is the directory where you installed the LCM Tools. For more information, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

b. Enter the following command:

```
./iamDeploymentWizard.sh
```

3. Review the Welcome screen to learn more about the Deployment wizard and to review the prerequisites.
4. If the Specify Inventory Directory screen appears:
   a. Click **OK** to accept the default location of the central inventory directory and the default Operating System Group Name for the directory.

      If the **Central Inventory Directory** field is empty, click Browse and select a local directory where your inventory of Oracle products will be stored.

   b. In the Inventory Location Confirmation dialog box, select **Continue Installation with local inventory**.

   If you want to create a central inventory directory or learn about the advantages of doing so, see Section 2.8.3.
5. On the Choose IAM Installation Option screen, select **Create a New Identity and Access Management Environment Deployment Response File**.
6. Use the Specify Security Updates screen to set up a notification preference for security-related updates and installation-related information from My Oracle Support. This information is optional.
   - **Email**: Specify your e-mail address to have updates sent by this method.
   - **I wish to receive security updates via My Oracle Support**: Select this option to have updates sent directly to your My Oracle Support account. You must enter your My Oracle Support Password if you select this option.
7. On the Describe Response File screen, specify descriptive information to identify the response file.

   The information entered on this screen is metadata information. It can be used to uniquely identify a response file if multiple response files are created.
   - **Response File Title**: Enter a new title for the response file or accept the default..
   - **Response File Version**: The Wizard provides a default value, which you can change. You can use this to keep track of different versions of the response file.
   - **Created By**: Defaults to the operating system user who invoked the Deployment Wizard. Set when the response file is initially created and cannot be modified for the current response file.
   - **Created Date**: Defaults to the date that the response file was initially created. Set when the response file was initially created and cannot be modified for the current response file.
   - **Response File Description**: Provide a description of this response file. This is an optional field.

8. Depending on the Oracle Identity and Access Management topology you're deploying, proceed to the appropriate section:
   - Section 4.3, "Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology"
   - Section 4.4, "Creating a Deployment Response File for an Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Topology"
   - Section 4.5, "Creating a Deployment Response File for an Integrated OIM, OAM, and OMSS Topology"

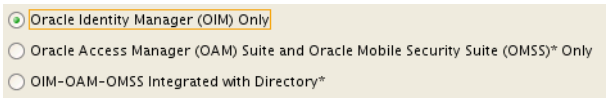
4.3 Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology

Complete the following steps to create a new Deployment Response File for an Oracle Identity Manager (OIM) Only topology:

Note: Single-host deployment using the Oracle Identity and Access Management Deployment Wizard is not meant for production use. This should be used for demonstrations and testing purposes only.

---

1. Perform the steps in Section 4.2, "Starting the Deployment Wizard and Navigating the Common Screens".
2. On the Suite Selection screen, select **Oracle Identity Manager (OIM) Only**.



Notes:

- After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection.

  If you need to make any modification in the previous screens, cancel and then restart the Oracle Identity and Access Management Deployment Wizard.

- The LCM Tools install and configure Oracle Mobile Security Suite only if the Operating System is Oracle Linux or RedHat Enterprise Linux.

  For specific operating system certifications, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page

---

3. On the Select Topology screen, select **Single Node**.

   In the **Host Name** field, specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.
4. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions.

For more information, see Section 4.6.1, "How To Specify the Installation and Configuration Locations in the Deployment Wizard".

5. Use the Configure Oracle HTTP Server screen to review or change the ports that will be used for the Oracle HTTP Server (OHS) instance.

   You should be able to use the default values for these ports, unless you have similar software running on the same host and you think there might be port conflicts.

   For more information about the fields on this screen, click **Help**.

6. Use the Configure Oracle Identity Manager screen to view or modify the ports that will be used by Oracle Identity Manager when you deploy the software.

   In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

   Optionally, select **Configure Email Server** if you want to identify and configure a mail server so Oracle Identity Management can send email notifications.

   For an explanation of each field, click **Help**.

7. Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains (or will contain) the required schemas.

   - If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do *not* select the **Create Schema Using RCU** check box.

     In this case, provide the details required to connect to the database where the schemas are installed, and then enter the password you created when you installed the schemas with RCU.

   - If you have not already installed the schemas, then select **Create Schema Using RCU**. This tells the LCM Tools to create the schemas for you as part of the deployment process.

     In this case, provide the details to connect to an existing, supported database. You must specify a user name with SYS privileges.

     In addition, you must provide a new password that will be used for all the newly created schemas, and an extra field appears so you can confirm the password.

   For more information, see Section 4.6.2, "Tips When Providing Database Connection Details in the Deployment Wizard".

8. Use the Configure SOA screen to enter the listen port for the SOA Managed server.

   - **SOA Host**: This field is purely informational and displays the host on which the product will run.
   - **Port**: Specify the port number to be used by the SOA Server.

9. Use the Configure Oracle Business Intelligence Publisher screen to enter the ports to be used by the BIP Managed server.

   - **BIP Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
   - **Port**: Specify the port number to be used by the BIP Server, for example: `9704`

10. Use the Set User Names and Passwords screen to set the passwords for the accounts that will be created during deployment.

You can set a common password for all of the user accounts listed, or you can set individual passwords for each of the accounts. It is also possible to change some of the default user names.

- To enter a common password for all the accounts to be created, enter the password in the Enter Common IAM Password field, and then re-enter the password in the **Confirm Common Password** field.
- If you want to create unique passwords for each account, then select the **Modify the Username and Password for the user accounts**, and select **Edit** next to the account you wish to modify.

11. Use the Summary screen to view a summary of your selections and enter additional information.
    - **Provisioning Response File Name**: Provide the name of the response file to be created. The default name of the deployment response file is `provisioning.rsp`. You can change this value.
    - **Provisioning Summary**: Provide the name of the deployment summary file to be created.
    - **Directory**: Specify the directory where you want this Deployment Response File to be saved.
12. Click **Finish** to exit the wizard.

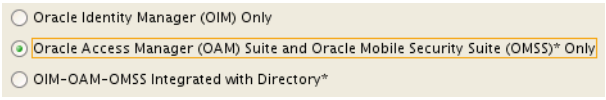
Note: The Identity and Access Management Deployment Wizard creates a deployment response file in the directory that you specify on the **Summary** screen. It also creates a folder named *responsefilename*_`data`, for example: `provisioning_data`. This folder contains the `cwallet.sso` file, which has encryption and decryption information.

If you move or copy the deployment response file to another location, you must also move or copy the *responsefilename*_`data` folder containing the `cwallet.sso` file to the same location.

4.4 Creating a Deployment Response File for an Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Topology

Complete the following steps to create a new Deployment Response File for a single-host Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) topology:

1. Perform the steps in Section 4.2, "Starting the Deployment Wizard and Navigating the Common Screens".
2. On the Select IAM Products screen, select **Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS)* Only**.



Notes:

- After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection.

  If you need to make any modification in the previous screens, cancel and then restart the Oracle Identity and Access Management Deployment Wizard.

- The LCM Tools install and configure Oracle Mobile Security Suite only if the Operating System is Oracle Linux or RedHat Enterprise Linux.

  For specific operating system certifications, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page

3. On the Directory Selection screen, do one of the following:

   - If you want to automatically create a new LDAP Directory Service using the LCM Tools, then select **Configure New Directory** and choose a directory type from the drop-down menu.
   - If you want to use an existing LDAP Directory service instance, then select **Use Existing Directory** and choose a directory type from the drop-down menu.

   Note: If you **Use Existing Directory**, then you must have previously prepared the directory for use with Oracle Identity and Access Management, using the procedures in Chapter 3.

4. On the Select Topology screen, select **Single Node**.

   In the **Host Name** field, specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.

5. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions.

   For more information, see Section 4.6.1, "How To Specify the Installation and Configuration Locations in the Deployment Wizard".

6. Use the Directory Configuration screen to provide details about the LDAP Directory service that will be used by the Oracle Identity and Access Management software you deploy.

   The fields on this screen vary depending on the Directory type you selected and whether you are using a new or existing Directory service:

   - If you selected the option to create a new LDAP Directory service instance, then use this screen to review or change the configuration settings that will be used when the Oracle Unified Directory or Oracle Internet Directory instance is created.
   - If you selected the option to use an existing LDAP Directory service instance, then use this screen to enter the details of existing instance.

For more information, see Section 4.6.3, "Tips When Providing Directory Service Information in the Deployment Wizard".

7. Use the Configure Oracle HTTP Server screen to review or change the ports that will be used for the Oracle HTTP Server (OHS) instance.

   You should be able to use the default values for these ports, unless you have similar software running on the same host and you think there might be port conflicts.

   For more information about the fields on this screen, click **Help**.

8. Use the Configure Oracle Access Manager screen to view or modify the ports that will be used by Oracle Access Manager when you deploy the software.

   In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

   For the **Cookie Domain** field, be sure to enter a domain address appropriate for your organization. Prefix the domain address with a leading period (.), for example:

   ```
   .example.com
   ```

   For an explanation of the other fields, click **Help**.

9. Use the Configure Oracle Mobile Security Manager screen to view or modify the ports that will be used by Oracle Mobile Security Manager when you deploy the software.

   In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

   For an explanation of the fields on the screen, click **Help**.

10. Use the Configure Oracle Mobile Security Access Server screen to view or modify the ports that will be used by Oracle Mobile Security Access Server when you deploy the software.

    In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

    For an explanation of the fields on this screen, click **Help**.

11. Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains (or will contain) the required schemas.

    - If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do *not* select the **Create Schema Using RCU** check box.

      In this case, provide the details required to connect to the database where the schemas are installed, and then enter the password you created when you installed the schemas with RCU.

    - If you have not already installed the schemas, then select **Create Schema Using RCU**. This tells the LCM Tools to create the schemas for you as part of the deployment process.

      In this case, provide the details to connect to an existing, supported database. You must specify a user name with SYS privileges.

      In addition, you must provide a new password that will be used for all the newly created schemas, and an extra field appears so you can confirm the password.

For more information, see Section 4.6.2, "Tips When Providing Database Connection Details in the Deployment Wizard".

12. Use the Set User Names and Passwords screen to set the passwords for the accounts that will be created during deployment.

    You can set a common password for all of the user accounts listed, or you can set individual passwords for each of the accounts. It is also possible to change some of the default user names.

    - To enter a common password for all the accounts to be created, enter the password in the Enter Common IAM Password field, and then re-enter the password in the **Confirm Common Password** field.
    - If you want to create unique passwords for each account, then select the **Modify the Username and Password for the user accounts**, and select **Edit** next to the account you wish to modify.

    If you are using an existing LDAP Directory service, then the **Credentials for Existing LDAP Users** section appears.

    This additional section lists the accounts and credentials that were created when you prepared the existing directory for use with Oracle Identity and Access Management, as described in Chapter 3.

13. Use the Summary screen to view a summary of your selections and enter additional information.

    - **Provisioning Response File Name**: Provide the name of the response file to be created. The default name of the deployment response file is `provisioning.rsp`. You can change this value.
    - **Provisioning Summary**: Provide the name of the deployment summary file to be created.
    - **Directory**: Specify the directory where you want this Deployment Response File to be saved.

14. Click **Finish** to exit the wizard.

Note: The Identity and Access Management Deployment Wizard creates a deployment response file in the directory that you specify on the **Summary** screen. It also creates a folder named *responsefilename*_`data`, for example: `provisioning_data`. This folder contains the `cwallet.sso` file, which has encryption and decryption information.

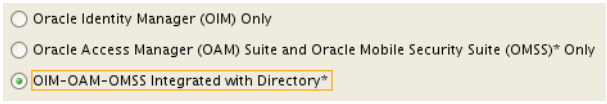
If you move or copy the deployment response file to another location, you must also move or copy the *responsefilename*_`data` folder containing the `cwallet.sso` file to the same location.

4.5 Creating a Deployment Response File for an Integrated OIM, OAM, and OMSS Topology

Complete the following steps to create a new Deployment Response File for a single-host Oracle Identity Manager (OIM), Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) with Directory topology:

Note: Single-host deployment using the Oracle Identity and Access Management Deployment Wizard is not meant for production use. This should be used for demonstrations and testing purposes only.

1. Perform the steps in Section 4.2, "Starting the Deployment Wizard and Navigating the Common Screens".
2. On the Select IAM Products screen, select **OIM-OAM-OMSS Integrated with Directory***.



Notes:

- After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection.

  If you need to make any modification in the previous screens, cancel and then restart the Oracle Identity and Access Management Deployment Wizard.

- The LCM Tools install and configure Oracle Mobile Security Suite only if the Operating System is Oracle Linux or RedHat Enterprise Linux.

  For specific operating system certifications, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page

3. On the Directory Selection screen, do one of the following:
   - If you want to automatically create a new LDAP Directory Service using the LCM Tools, then select **Configure New Directory** and choose a directory type from the drop-down menu.
   - If you want to use an existing LDAP Directory service instance, then select **Use Existing Directory** and choose a directory type from the drop-down menu.

   Note: If you **Use Existing Directory**, then you must have previously prepared the directory for use with Oracle Identity and Access Management, using the procedures in Chapter 3.

4. On the Select Topology screen, select **Single Node**.

   In the **Host Name** field, specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.

5. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions.

For more information, see Section 4.6.1, "How To Specify the Installation and Configuration Locations in the Deployment Wizard".

6. Use the Directory Configuration screen to provide details about the LDAP Directory service that will be used by the Oracle Identity and Access Management software you deploy.

   The fields on this screen vary depending on the Directory type you selected and whether you are using a new or existing Directory service:

   - If you selected the option to create a new LDAP Directory service instance, then use this screen to review or change the configuration settings that will be used when the Oracle Unified Directory or Oracle Internet Directory instance is created.
   - If you selected the option to use an existing LDAP Directory service instance, then use this screen to enter the details of existing instance.

   For more information, see Section 4.6.3, "Tips When Providing Directory Service Information in the Deployment Wizard".

7. Use the Configure Oracle HTTP Server screen to review or change the ports that will be used for the Oracle HTTP Server (OHS) instance.

   You should be able to use the default values for these ports, unless you have similar software running on the same host and you think there might be port conflicts.

   For more information about the fields on this screen, click **Help**.

8. Use the Configure Oracle Identity Manager screen to view or modify the ports that will be used by Oracle Identity Manager when you deploy the software.

   In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

   Optionally, select **Configure Email Server** if you want to identify and configure a mail server so Oracle Identity Management can send email notifications.

   For an explanation of each field, click **Help**.

9. Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains (or will contain) the required schemas.

   - If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do *not* select the **Create Schema Using RCU** check box.

     In this case, provide the details required to connect to the database where the schemas are installed, and then enter the password you created when you installed the schemas with RCU.

   - If you have not already installed the schemas, then select **Create Schema Using RCU**. This tells the LCM Tools to create the schemas for you as part of the deployment process.

     In this case, provide the details required to connect to an existing, supported database, and then provide a new password that will be created for all the schemas. In this scenario, an extra field appears so you can enter the password again in the **Confirm Schema Password** field.

   For more information, see Section 4.6.2, "Tips When Providing Database Connection Details in the Deployment Wizard".

10. Use the Configure SOA screen to enter the listen port for the SOA Managed server.

- **SOA Host**: This field is purely informational and displays the host on which the product will run.
- **Port**: Specify the port number to be used by the SOA Server.

11. Use the Configure Oracle Business Intelligence Publisher screen to enter the ports to be used by the BIP Managed server.
    - **BIP Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
    - **Port**: Specify the port number to be used by the BIP Server, for example: `9704`
12. Use the Configure Oracle Access Manager screen to view or modify the ports that will be used by Oracle Access Manager when you deploy the software.

    In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

    For the **Cookie Domain** field, be sure to enter a domain address appropriate for your organization. Prefix the domain address with a leading period (.), for example:

    ```
    .example.com
    ```

    For an explanation of the other fields, click **Help**.
13. Use the Configure Oracle Mobile Security Manager screen to view or modify the ports that will be used by Oracle Mobile Security Manager when you deploy the software.

    In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

    For an explanation of the fields on the screen, click **Help**.
14. Use the Configure Oracle Mobile Security Access Server screen to view or modify the ports that will be used by Oracle Mobile Security Access Server when you deploy the software.

    In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

    For an explanation of the fields on this screen, click **Help**.
15. Use the Configure Access Policy Manager screen to view or modify the ports that will be used by the Access Policy Manager when you deploy the software.

    In most cases you can leave the default values, unless you have similar software running on the same host and you think there might be port conflicts.

    For an explanation of the fields on this screen, click **Help**.
16. Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains (or will contain) the required schemas.
    - If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do *not* select the **Create Schema Using RCU** check box.

      In this case, provide the details required to connect to the database where the schemas are installed, and then enter the password you created when you installed the schemas with RCU.

- If you have not already installed the schemas, then select **Create Schema Using RCU**. This tells the LCM Tools to create the schemas for you as part of the deployment process.

  In this case, provide the details required to connect to an existing, supported database, and then provide a new password that will be created for all the schemas. In this scenario, an extra field appears so you can enter the password again in the **Confirm Schema Password** field.

For more information, see Section 4.6.2, "Tips When Providing Database Connection Details in the Deployment Wizard".

17. Use the Set User Names and Passwords screen to set the passwords for the accounts that will be created during deployment.

    You can set a common password for all of the user accounts listed, or you can set individual passwords for each of the accounts. It is also possible to change some of the default user names.

    - To enter a common password for all the accounts to be created, enter the password in the Enter Common IAM Password field, and then re-enter the password in the **Confirm Common Password** field.
    - If you want to create unique passwords for each account, then select the **Modify the Username and Password for the user accounts**, and select **Edit** next to the account you wish to modify.

    If you are using an existing LDAP Directory service, then the **Credentials for Existing LDAP Users** section appears.

    This additional section lists the accounts and credentials that were created when you prepared the existing directory for use with Oracle Identity and Access Management, as described in Chapter 3.

18. The Summary screen appears.

    Use the Summary screen to view a summary of your selections and enter additional information.

    - **Provisioning Response File Name**: Provide the name of the response file to be created. The default name of the deployment response file is `provisioning.rsp`. You can change this value.
    - **Provisioning Summary**: Provide the name of the deployment summary file to be created.
    - **Directory**: Specify the directory where you want this Deployment Response File to be saved.

19. Click **Finish** to exit the wizard.

Note: The Identity and Access Management Deployment Wizard creates a deployment response file in the directory that you specify on the **Summary** screen. It also creates a folder named *responsefilename*_`data`, for example: `provisioning_data`. This folder contains the `cwallet.sso` file, which has encryption and decryption information.

If you move or copy the deployment response file to another location, you must also move or copy the *responsefilename*_`data` folder containing the `cwallet.sso` file to the same location.

4.6 Additional Information When Creating a Response File for an Automated Deployment

The following sections provide supporting information when you are using the Deployment Wizard to create a response file in preparation for an automated deployment of Oracle Identity and Access Management:

- Section 4.6.1, "How To Specify the Installation and Configuration Locations in the Deployment Wizard"
- Section 4.6.2, "Tips When Providing Database Connection Details in the Deployment Wizard"
- Section 4.6.3, "Tips When Providing Directory Service Information in the Deployment Wizard"

4.6.1 How To Specify the Installation and Configuration Locations in the Deployment Wizard

When you are using the Deployment Wizard, you are prompted to identify important directory locations that the LCM Tools will use when it automatically installs and configures your Oracle Identity and Access Management software.

Use the following steps to fill out the Installation and Configuration Locations screen in the Deployment Wizard:

1. In the **Life Cycle Management Store Location** field, enter the path to a new directory that will be created to store information required by the LCM tools.

   The LCM Tools will use the information here to keep track of the topology you configure (via the `topology.xml` file), logs of LCM Tool sessions, and other LCM Tool-specific artifacts.

   Choose a location outside the Middleware home that will be accessible when you later perform other life cycle actions, such as patching and upgrade. This location is also known as the LCM_STORE.

2. In the **Software Repository Location** field, enter the path to the existing directory where you unpacked the repository archives.

   This directory contains all the Oracle Identity and Access Management installers.

   The Wizard will check to be sure there is an `installers` folder inside this directory. This location is also known as the REPOS_HOME.

3. In the **Software Installation Location** field, enter the path to a new directory that will contain the Oracle home directories where the LCM Tools install the software binaries.

   This directory is also known as the IDMTOP directory. When you deploy the software, the LCM Tools will automatically create a `products` folder inside the IDMTOP directory. The `IDMTOP/products` folder will contain the Middleware home for the Oracle Identity and Access Management software you install.

4. In the **Shared Configuration Field**, enter the path to a new directory that will contain all the domain configuration information for your Oracle Identity and Access Management software.

   By default, the Wizard assumes this directory is inside the IDMTOP directory, but you can specify the path to a new directory in any accessible location.

For more information, refer to the following:

- Section 4.2, "Starting the Deployment Wizard and Navigating the Common Screens"
- Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure"

4.6.2 Tips When Providing Database Connection Details in the Deployment Wizard

When you are using the Deployment Wizard, you are prompted to provide details that allow the LCM Tools to connect to a supported database. It will use this information to access existing schemas you installed previously or to install the schemas automatically.

When you are providing database connection details in the Deployment Wizard, note the following:

- If you have not already created the schemas, be sure the Database user name you enter in the **SYSDBA Username** field has SYS privileges.

  The Deployment Wizard needs these privileges in order to create the schemas in the database.

- In the **Service Name** field, be sure to enter the full service name of the database, including the domain. For example: `oimdb.example.com`
- When entering a value in the **Schema Prefix** field, note the following:
  - The Schema Prefix is required so you can easily locate in the database the schemas required for the current domain. All schemas created in this session will use this prefix.
  - If you are have already created the schemas in the database before running the Deployment Wizard, then enter the prefix you used when you created the schemas in RCU.
  - If you did not already create the schemas, then enter a new prefix that will be used for all the schema names that the LCM Tools create when you deploy the software.
  - As an example, the default value of the **Schema Prefix** field field is `EDGIGD` (for Oracle Identity Management governance domains) and `EDGIAD` (for Oracle Access Manager access domains).
  - The value you enter in the **Schema Prefix** field will automatically be added to the standard schema name in the **Schema Name** field.

4.6.3 Tips When Providing Directory Service Information in the Deployment Wizard

When you are using the Deployment Wizard, you are prompted to provide details that allow the LCM Tools to create or connect to a supported LDAP Directory service.

When you are providing this information on the Directory Configuration screen of the Deployment Wizard, note the following:

- Be sure to review all the editable fields to be sure they reflect the values required for your organization.

  In particular, note that the **Container Details** section of the screen includes "example" values for the realm. Be sure to replace with these values with the Distinguished Name of the realm for your organization.

- Values for fields that are not editable were determined by the Deployment Wizard, based on the information you provided when you selected the products and topology options earlier in the Wizard.
- Be sure to indicate whether or not you are using secure (SSL) communications for the Directory service ports.

  For example, for a Microsoft Active Directory instance, you must provide SSL information if you are deploying the integrated OIM, OAM, and OMSS topology.

  For Oracle Unified Directory (OUD) or Oracle Internet Directory (OID), provide a non-SSL port for communications.
- If you are creating an Oracle Internet Directory (OID) instance, then three additional port fields are shown, all related to the Oracle Process Manager and Notification Server (OPMN). OPMN is used to manage the OID instance.

  You can typically use the default values for these ports, unless you have other OPMN-managed products running on the same system, which would cause potential port conflicts:

  - OPMN Local Port
  - OPMN Remote Port
  - OPMN Request Port

5

Performing Oracle Identity and Access Management Deployment

After creating the deployment response file, use it to deploy the Oracle Identity and Access Management environment. This chapter describes how to deploy Oracle Identity and Access Management.

This chapter contains the following sections:

- Section 5.1, "Understanding the Stages of an Oracle Identity Management Automated Deployment"
- Section 5.2, "About the Services and Servers Configured in Each Deployment Phase"
- Section 5.3, "Manual Deployment Tasks When Using Microsoft Active Directory for an Integrated Topology"
- Section 5.4, "Running the Environment Health Check Utility Before Deployment"
- Section 5.5, "Deploying Oracle Identity and Access Management Using the LCM Tools"
- Section 5.6, "Reviewing Environment Health Check Utility Reports and Logs After Deployment"

5.1 Understanding the Stages of an Oracle Identity Management Automated Deployment

When you use the LCM tools to deploy an Oracle Identity and Access Management environment, you run the deployment in stages. At the end of each stage, you can verify that the stage has completed successfully before advancing to the next stage.

To better prepare for and understand the automatic deployment process, Table 5–1 lists the deployment stages for an integrated Oracle Identity Management, Oracle Access Manager, and Oracle Mobile Security Services deployment.

To give you an idea how long each stage can take to finish, the table also provides a time estimate for each stage when you are installing and deploying the integrated environment.

Note: The specific time required for each stage will vary, depending upon the topology you have selected, whether you are using an existing LDAP directory or creating new one, and other factors, such as available system resources.

Table 5–1 Summary of the Phases for an Integrated OIM-OAM-OMSS Deployment

Phase Number	Phase Name	Description	Estimated Duration
1	Preverify	Verifies that the minimum prerequisites are met. For this phase, the LCM Tools use the Oracle Identity and Access Management Health Check Utility to check for various system requirements, including: ■ Available ports ■ Connection to the database ■ Free disk space ■ Physical and Virtual Memory For more information about the items verified by the Health Check Utility, see *Verifying Your Oracle Identity and Access Management Environment*. If any mandatory plugins (plugins that check for mandatory parameters in the environment for the provisioning to be successfully completed) fail, it will stop you from going forward with the provisioning. If any optional plugins (plugins that check for recommended but not mandatory parameters in the environment) fail, it will warn you but you can still go forward with the provisioning by ignoring the warning. For more information, see "Analyzing Health Check Reports" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.	1 minute
2	Install	Invokes the required installers in the software repository, creates the required Middleware home directories, installs the software binary files on disk, and applies any required patches to the binary files.	75 minutes

Table 5–1 (Cont.) Summary of the Phases for an Integrated OIM-OAM-OMSS Deployment

Phase Number	Phase Name	Description	Estimated Duration
3	Preconfigure	Performs the following tasks in preparation for configuring the software: **1.** If you have chosen to have the LCM tools install the schemas, then the LCM Tools run the Repository Creation Utility (RCU) to create the required schemas in the database. **2.** If you have chosen to create a new LDAP Directory Service as part of the automated deployment, then the LCM Tools configure an Oracle Unified Directory or Oracle Internet Directory instance. **3.** Adds the required users and groups to the new LDAP Directory Service instance. **4.** Creates the initial Oracle WebLogic Server domains (IAMAccessDomain and IAMGovernanceDomain). **5.** Extends the Access domain with the following products: ■ Oracle Access Manager (OAM) ■ Oracle Mobile Security Manager (OMSM) ■ The Unified User Interface ■ Application Provisioning Manager (APM) **6.** Extends the Governance domain with the following products: ■ Oracle Identity Manager (OIM) ■ Oracle SOA Suite ■ Oracle Business Intelligence Publisher (BIP) ■ Application Provisioning Manager (APM) **7.** Configures Oracle HTTP Server.	75 Minutes

Table 5–1 (Cont.) Summary of the Phases for an Integrated OIM-OAM-OMSS Deployment

Phase Number	Phase Name	Description	Estimated Duration
4	Configure	Configures the software by performing the following steps: 1. Configures the Node Manager for the domain. 2. Runs the Oracle Identity Management Configuration Wizard to create the OIM artifacts. 3. Runs the idmConfigTool with the `-configOAM` argument to perform the following tasks: ▪ Create the Oracle WebLogic Server authenticators ▪ Create the LDAP Identity Store ▪ Create the WebGate profiles (Webgate_IDM, Webgate_IDM_11g) 4. Runs the idmConfigTool with the `-configOMSS mode=OMSM` argument to configure Oracle Mobile Security Services (OMSS). 5. Create the OMSAS instance. 6. Run the idmConfigTool with the `-configOMSS mode=OMSAS` argument.	40 Minutes
5	Configure - secondary	Performs some required secondary configuration tasks: 1. Exports the OMSS certificates into Governance domain. 2. Runs the idmConfigTool with the -configOIM argument, which performs the following tasks for Oracle Identity Manager: ▪ Creates the Oracle WebLogic Server authenticators. ▪ Performs the TAP registration. ▪ Adds the necessary CSF entries to the keystore for NAP configuration. ▪ Integrates Oracle Identity Management and Oracle Access Manager.	20 Minutes
6	PostConfigure	Performs the following post-configuration tasks: 1. Tunes the software to meet performance standards. 2. Configures the email server (if you selected this option while creating the response file). 3. Creates and configures the `weblogic_idm` user, which is the default administration account for the domains. 4. Configures the Federation software for Oracle Access Manager. 5. Registers the Oracle HTTP Server instance with the Access domain 6. Configures Webgate.	40 Minutes

Table 5–1 (Cont.) Summary of the Phases for an Integrated OIM-OAM-OMSS Deployment

Phase Number	Phase Name	Description	Estimated Duration
7	Startup	Starts all the servers and services.	45 Minutes
8	Validate	Validates the deployment using the Oracle Identity and Access Management Health Check Utility. The status of post install Health Check utility plugins are available at the following location: `LCMDIR/provisioning/logs/<host name>/healthcheck-error/logs/healthchecker`	2 Minutes

5.2 About the Services and Servers Configured in Each Deployment Phase

If a deployment fails during one of the phases, you can use the Cleanup and Restore to roll back the deployment to the end of the Install phase. Alternatively, you can also stop the deployment at the end of each phase and back up the environment. That way, if the next phase should fail, you can easily restore your environment to its state at the end of the last successful deployment phase.

However, before you can back up your environment, you must first stop any servers or processes that are running and then restart them when the backup is complete.

Table 5–2 provides a list of servers and processes that you need to stop before you back up each phase of the deployment and then start again when the backup is complete.

The names of the Managed Servers in Table 5–2 can vary, depending on the names you selected for each server. However, for the purposes of this guide, the Managed Servers use the names shown in the topology diagrams in Section 1.3, "Oracle Identity and Access Management Topologies Supported by the LCM Tools".

Table 5–2 List of Servers to Stop Before Backing Up after Each Provisioning Phase

	Phase	OIM Deployment	OAM and OMSS with OUD[1] Deployment	Integrated, OIM, OAM, OMSS, and OUD Deployment
1	Preverify	None	None	None
2	Install	None	None	None
3	Preconfigure	Node Manager Administration Server Oracle HTTP Server	Oracle Unified Directory (OUD) Node Manager Administration Server Oracle HTTP Server	OUD Node Manager Access Administration Server Governance Administration Server Oracle HTTP Server

Table 5–2 (Cont.) List of Servers to Stop Before Backing Up after Each Provisioning Phase

	Phase	OIM Deployment	OAM and OMSS with OUD[1] Deployment	Integrated, OIM, OAM, OMSS, and OUD Deployment
4	Configure	Node Manager Administration Server Oracle HTTP Server wls_oim1	OUD Node Manager Administration Server Oracle HTTP Server wls_oam1 wls_msm1	OUD Node Manager Access Administration Server wls_oam1 wls_msm1 Governance Administration Server wls_oim1 Oracle HTTP Server
5	Configure - Secondary	.Node Manager Administration Server Oracle HTTP Server wls_oim1	OUD Node Manager Administration Server Oracle HTTP Server wls_oam1 wls_msm1	OUD Node Manager Access Administration Server wls_oam1 wls_msm1 Governance Administration Server wls_oim1 Oracle HTTP Server
6	Postconfigure	Node Manager Administration Server Oracle HTTP Server wls_oim1 wls_soa1	OUD Node Manager Administration Server Oracle HTTP Server wls_oam1 wls_msm1	OUD Node Manager Access Administration Server wls_oam1 wls_msm1 Governance Administration Server wls_oim1 wls_soa1 Oracle HTTP Server
7	Startup	Node Manager Administration Server Oracle HTTP Server wls_oim1 wls_soa1 wls_bi1	OUD Node Manager Administration Server Oracle HTTP Server wls_oam1 wls_msm1 wls_ama1 MSAS	OUD Node Manager Access Administration Server wls_oam1 wls_msm1 wls_ama1 Governance Administration Server wls_oim1 wls_soa1 wls_bi1 MSAS Oracle HTTP Server

Table 5–2 (Cont.) List of Servers to Stop Before Backing Up after Each Provisioning Phase

	Phase	OIM Deployment	OAM and OMSS with OUD[1] Deployment	Integrated, OIM, OAM, OMSS, and OUD Deployment
8	validate	Node Manager	OUD	OUD
		Administration Server	Node Manager	Node Manager
		Oracle HTTP Server	Administration Server	Access Administration Server
		wls_oim1	Oracle HTTP Server	wls_oam1
		wls_soa1	wls_oam1	wls_msm1
		wls_bi1	wls_msm1	wls_ama1
			wls_ama1	Governance Administration Server
			MSAS	wls_oim1
				wls_soa1
				wls_bi1
				MSAS
				Oracle HTTP Server

[1] This table assumes you are deploying an Oracle Unified Directory (OUD) instance; if you are deploying an Oracle Internet Directory (OID) instance, then replace any references to OUD with OID.

5.3 Manual Deployment Tasks When Using Microsoft Active Directory for an Integrated Topology

If you are using an existing Microsoft Active Directory instance as part of your Oracle Identity and Access Management deployment, then there are two important steps you must perform during and after the Oracle Identity and Access Management deployment.

These steps apply only if are using Active Directory and you are deploying the integrated OIM, OAM, and OMSS topology:

- Section 5.3.1, "Extending the OIM Schema for Active Directory After the Install Phase"
- Section 5.3.2, "Disabling the LDAPAddMissingObjectClasses Event Handler After the Configure Phase"

5.3.1 Extending the OIM Schema for Active Directory After the Install Phase

If you are using Active Directory as part of an integrated OIM, OAM, and OMSS deployment, then you must perform the following procedure after the Install phase completes successfully and before the Preconfigure phase:

1. Change directory to the following directory in the Middleware home, which was created during the Install phase:

   ```
   cd MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates/
   ```

   This directory contains the `extendsadschema` script, which automatically loads the following LDIF files, which are also installed into the `oimtemplates` directory:

   - `adOAMDisable.ldif`
   - `adOAMEnable.ldif`
   - `adOIMLanguageSubtype.ldif`

- adOIMSchema.ldif

2. Run the following command to extend Active Directory schema:

```
./extendadschema.sh
    -h AD_host
    -p AD_port
    -D administrator@example.com
    -AD dc=example,dc=com>
    -OAM true
```

Note: The extendadschema script is certified only for Active Directory 2003, 2008, 2008R2, and 2012.

5.3.2 Disabling the LDAPAddMissingObjectClasses Event Handler After the Configure Phase

If you are using Active Directory as part of an integrated OIM, OAM, and OMSS deployment, then you should disable the LDAPAddMissingObjectClasses Oracle Identity Management event handler after the **Configure** or **Configure - Secondary** phase and before the **Post-Configure** phase.

For more information, see "Disabling the LDAPAddMissingObjectClasses for Users and Roles" in the *Integration Guide for Oracle Identity Management Suite*.

Be sure to restart the OIM Managed Server after you complete this task.

5.4 Running the Environment Health Check Utility Before Deployment

Before you deploy Oracle Identity and Access Management using the Deployment Wizard, Oracle recommends that you run the Environment Health Check Utility to verify that your environment meets the minimum requirements for running the deployment wizard and deploying the software.

To perform the system verification before deploying Oracle Identity and Access Management:

1. Set the JAVA_HOME environment variable to the full path of your JDK directory.
2. Change directory to the following directory where you downloaded and unpacked the Environment Health Check Utility:

```
cd IDMLCM_HOME/healthcheck/bin
```

3. Run the following command to perform the pre-installation validation checks:

```
./idmhc.sh -manifest ../config/PreInstallChecks_mandatory_manual.xml
```

Note: For more information about the pre-installation checks performed by the Environment Health Check Utility, see "PreInstallChecks_mandatory_manual.xml" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.

4. If any health checks fail, refer to the output in the Health Check Utility log files and reports to find the corrective actions. Note that the log file location will be printed on the screen after the utility is executed.

The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful. For more information about the log files and reports, see "Analyzing Health Check Reports" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.

5.5 Deploying Oracle Identity and Access Management Using the LCM Tools

After you have created a response file, you can deploy the Oracle Identity and Access Management software using the deployment tool command line or the Oracle Identity and Access Management Deployment Wizard.

Note: Before you start the deployment, make sure all unnecessary processes are shut down on the host. One way to do this is to reboot the host before performing Oracle Identity and Access Management deployment.

This section contains the following topics:

- Section 5.5.1, "Deploying Oracle Identity and Access Management Using the Deployment Wizard"
- Section 5.5.2, "Deploying Oracle Identity and Access Management Using the LCM Tools Command Line"

5.5.1 Deploying Oracle Identity and Access Management Using the Deployment Wizard

If you want to use the Oracle Identity and Access Management Deployment Wizard to perform deployment,

1. Ensure that the environment JAVA_HOME variable is set to the directory where you unpacked the `jdk.zip` file from the installers directory in the software repository.

   For example:

   REPOS_HOME`/jdk`.

2. Start the Oracle Identity and Access Management Deployment Wizard, as follows:

   ```
   cd IDMLCM_HOME/provisioning/bin
   ./iamDeploymentWizard.sh
   ```

3. On the Choose IAM Installation Options screen:

   a. Select **Deploy an Identity and Access Management Environment**.

   b. In the **Response File** field, specify the path name of the file you want to use, either by typing it in the field or by clicking the **Browse** button, navigating to the desired file, and selecting it.

      This is the deployment response file that you created in Chapter 4, "Creating a Deployment Response File."

4. On the Describe Response File screen, review the information about the response file that you created earlier as part of the Deployment Profile.

For more information, see 5 in Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology.

5. On the Select Installation and Configuration Locations screen, review the information about the Oracle Identity and Access Management installation and configuration directories that you had provided when creating the Deployment Profile.

   For more information, see 9 in Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology.

6. On the Review Deployment Configuration screen, select the configurations you want to review.

   This is an optional step. If you want to view or modify the configuration details of any component, then select that component and click **Next**. Based on the options that you select, the corresponding configuration screens are displayed.

   - OUD Configuration
   - OHS Configuration
   - SOA Configuration
   - OIM Configuration
   - OAM Configuration
   - OIM DB Configuration
   - OAM DB Configuration

7. On the Summary screen, review your selections to ensure that the installation details are what you intend.

   Click **Next** to start the deployment process. The wizard displays a screen for each phase of the deployment process. Each screen corresponds to the phases described in Section 5.1.

8. Monitor the Wizard screens to track the progress of the deployment process.

   The status icon at the top of screen shows the status of the stage:

   - **The block icon** indicates that processing of the current stage has not yet started.
   - **The clock icon** indicates that the current stage is in progress.
   - **The green check mark** indicates that the current stage completed successfully.

     When a stage finishes successfully, the Wizard pauses until you click **Next** to advance to the next stage.
   - **An "x" icon in a red circle** indicates that the current stage has failed. You must correct the errors before you can continue.

     Click the **x** icon to display information about the failures. Click a **Log** file to see details specific to the stage.

     For information about how to recover from a failed stage, see Appendix A, "Cleaning Up an Environment Before Rerunning IAM Deployment".

9. At the end of each successful stage, consider backing up the environment.

If you back up your environment after each phase and a stage fails, then you can easily restore your environment to the state it was in after the last successful stage. For more information, see Section 5.2, "About the Services and Servers Configured in Each Deployment Phase".

> **Note:** If you are using Microsoft Active Directory for an integrated deployment, then there are mandatory steps you must perform on the directory after the Install phase and after the Configure phase.
>
> For more information, see Section 5.3, "Manual Deployment Tasks When Using Microsoft Active Directory for an Integrated Topology".

10. If all deployment stages are successful, the Wizard displays the Install Complete screen, which shows a summary of the products that have been installed and configured.

    Click **Finish** to save the summary and exit the Oracle Identity and Access Management Deployment Wizard.

5.5.2 Deploying Oracle Identity and Access Management Using the LCM Tools Command Line

To use the command line deployment tool, you must run the `runIAMDeployment.sh` script a number of times, specifying the deployment stage with the `-target` option. You MUST complete each command, in order, before running the next command.

> **Note:** If you are using Microsoft Active Directory for an integrated deployment, then there are mandatory steps you must perform on the directory after the Install phase and after the Configure phase.
>
> For more information, see Section 5.3, "Manual Deployment Tasks When Using Microsoft Active Directory for an Integrated Topology".

Before running the deployment tool, ensure that the environment variable `JAVA_HOME` is set to the directory where *`REPOS_HOME`*`/installers/jdk/jdk.zip` was extracted. For example, *`REPOS_HOME`*`/jdk`.

The command syntax for the deployment tool on UNIX is:

```
runIAMDeployment.sh -responseFile RESPONSE_FILE -target STAGE
```

In this example, note the following:

- *`RESPONSE_FILE`* is the complete path to the location of the deployment response file. You specified the file name and directory on the **Summary** screen when you ran the wizard to create the deployment response file.

  On Unix, the default value is:

  `IDMLCM_HOME``/provisioning/bin/provisioning.rsp`

- It is important that you perform the deployment commands for each deployment phase in the correct order.

  For example, review Example 5–1, which shows each of the commands in the proper order, by deployment phase.

Example 5–1 Example of Running the LCM Tools Command Line Actions for a Complete Deployment

```
runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target preverify

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target install

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target
preconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target configure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target
configure-secondary

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target
postconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target startup

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp -target validate
```

5.6 Reviewing Environment Health Check Utility Reports and Logs After Deployment

After you finish automatic deployment Oracle Identity and Access Management using the LCM Tools, review the log files and reports that were generated by the Oracle Identity and Access Management Environment Health Check Utility.

The log files and HTML reports are saved to the following location during a deployment with the LCM Tools:

IDMLCM_HOME/healthcheck/bin/logs/healthchecker/

The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful.

For more information about the log files and reports, see "Analyzing Health Check Reports" in *Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment*.

Note for HP-UX Users: The following error in the logs or HTML reports can be safely ignored:

```
ERROR: OIMHC-20024: SOAConfigCheck plugin failed.
OIMHC-20137: Error occurred while trying to authenticate the user
"weblogic_idm". Ensure that the configuration is correct.
```

To validate the deployment, use the standard validation URLs provided in Chapter 7

Part III

Post-Deployment Tasks and Troubleshooting

Part III provides information about the post-deployment tasks. It also provides information on troubleshooting Oracle Identity and Access Management deployment.

Part III contains the following chapters:

- Chapter 6, "Post Deployment Tasks"
- Chapter 7, "Validating Deployment"
- Chapter 8, "Troubleshooting Oracle Identity and Access Management Deployment"

6

Post Deployment Tasks

This chapter describes tasks you must perform after you have completed Oracle Identity and Access Management Deployment.

This chapter contains the following sections:

- Section 6.1, "Post Deployment Task for Accessing Help on the WebLogic Administration Console"
- Section 6.2, "Starting and Stopping Oracle Identity and Access Management Components After an Automated Deployment"

6.1 Post Deployment Task for Accessing Help on the WebLogic Administration Console

To access help on the WebLogic Administration Console, you must complete the following steps:

> **Note:** This section is not applicable if you have created the OIM only topology by performing tasks listed in Creating a Deployment Response File for an Oracle Identity Manager (OIM) Topology.

1. Log in to the Oracle Access Manager Console using the following URL:

   `http://hostname:port/oamconsole`

2. In the **Access Manager** pane, click on **Application Domains**.
3. A **Search Application Domains** tab opens. In the Name field, enter **IAM Suite**, and click on **Search**.
4. In the **Search Results**, click on **IAM Suite**.
5. Click on the **Resources** tab.
6. Click on **New Resource** and enter the following information:
   - **Type**: HTTP
   - **Description**: All resources for WLS console help
   - **Host Identifier**: IAMSuiteAgent
   - **Resource URL**: /consolehelp/**
   - **Query**: Name Value list
   - **Operations Available**: All

- **Protection Level**: Excluded

7. Click on **Apply**.

6.2 Starting and Stopping Oracle Identity and Access Management Components After an Automated Deployment

At the end of the Oracle Identity and Access Management automated deployment, all the domains and software are started automatically.

However, if you later need to stop or restart the environment, then it is important that you use the provided start and stop scripts, which stop and start the various components of the deployment in the required order.

For more information, see the following topics:

- Section 6.2.1, "Starting and Stopping Components Using the Provided Start and Stop Scripts"
- Section 6.2.2, "Starting and Stopping Components Manually"

6.2.1 Starting and Stopping Components Using the Provided Start and Stop Scripts

The following sections provide information about the provided start and stop scripts that you can use to start and stop the Oracle Identity and Access Management software after an automated deployment:

- Section 6.2.1.1, "Locating the Provided Start and Stop Scripts"
- Section 6.2.1.2, "About Password Management When Using the Start and Stop Scripts"
- Section 6.2.1.3, "Starting Components Using the Provided Scripts"
- Section 6.2.1.4, "Stopping Components Using the Provided Scripts"
- Section 6.2.1.5, "Optional Arguments When Using the Start and Stop Scripts"
- Section 6.2.1.6, "Changing the Passwords in the credconfig Wallet"

6.2.1.1 Locating the Provided Start and Stop Scripts

After you complete an automated installation of Oracle Identity Management with the LCM Tools, a set of scripts are installed in the configuration directory. Based on the recommended directory structure, the scripts are installed in the following directory:

```
IDMTOP/config/scripts/
```

For more information about the standard directories in an LCM Tools automated installation, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

Inside the scripts folder, you should find two scripts:

```
startall.sh
stopall.sh
```

6.2.1.2 About Password Management When Using the Start and Stop Scripts

The command line for using the provided start and stop scripts has an optional argument for entering the password for the domain administrator account.

However, this argument is not required because, by default, the passwords required to start and stop the Oracle Identity and Access Management components is saved in a secure wallet file. The wallet file is referenced automatically by the start and stop scripts, so there is no need to enter the password on the command line.

The wallet file used by the start and stop scripts (`cwallet.sso`) is located in the following directory after an automated deployment:

LCM_STORE`/lcmconfig/config/credconfig/`

For information about changing the value of the password in the wallet file, see Section 6.2.1.6.

6.2.1.3 Starting Components Using the Provided Scripts

To stop all the Oracle Identity and Access Management components after an automated deployment:

1. Change directory to the scripts directory in the shared configuration directory.

   For example:

   ```
   cd IDMTOP/config/scripts
   ```

2. Run the script as follows:

   ```
   sh startall.sh
   ```

6.2.1.4 Stopping Components Using the Provided Scripts

To stop all the Oracle Identity and Access Management components after an automated deployment:

1. Change directory to the scripts directory in the shared configuration directory.

   For example:

   ```
   cd IDMTOP/config/scripts
   ```

2. Run the script as follows:

   ```
   sh stopall.sh
   ```

6.2.1.5 Optional Arguments When Using the Start and Stop Scripts

In most cases, you don't need to enter any arguments to the start and stop scripts. However, if necessary, Table 6–1 lists the optional arguments can be used when running the scripts.

Table 6–1 Optional Arguments When Using the Start and Stop Scripts

Argument	Description	Example
domain_name=	Allows you to specify a specific domain. When you use this argument, only components in the specified domain will be started.	sh startall domain=IAMAccessDomain

Table 6–1 (Cont.) Optional Arguments When Using the Start and Stop Scripts

Argument	Description	Example
weblogic_pwd=	Allows you to enter the weblogic administration password on the command line. Note that Oracle recommends that you do not enter clear passwords on the command line and instead use the wallet file provided by the LCM Tools. For more information, see Section 6.2.1.6.	sh startall weblogic_pwd=*mypassword*
nodemanager_pwd=	Allows you to enter the Node Manager password on the command line. Note that Oracle recommends that you do not enter clear passwords on the command line and instead use the wallet file provided by the LCM Tools. For more information, see Section 6.2.1.6.	sh startall nodemanager_pwd=*my_nm_password*
-help	Displays online help that describes the usage of the script.	sh startall -help

6.2.1.6 Changing the Passwords in the credconfig Wallet

If you change the Oracle WebLogic Server administration password or the Node Manager password after you perform an automated deployment, you can update the passwords stored in the start and stop script wallet:

1. Change directory to the directory where the wallet resides:

   ```
   cd LCM_STORE/lcmconfig/credconfig/
   ```

2. Display the list of keys in the wallet and the credentials for each key:

   ```
   sh csf-util.sh list
   ```

3. Change the password for one of the keys in the wallet:

   ```
   sh csf-util.sh add
   ```

   The script prompts you for the name of the key, the user, and then for the new password.

6.2.2 Starting and Stopping Components Manually

Oracle recommends that you use the scripts provided by the LCM Tools to start and stop the Oracle Identity Management components after an automated deployment.

However, if there are situations where you cannot run the provided scripts, refer to the following topics before attempting to manually start or stop the Oracle Identity and Access Management components:

- Section 6.2.2.1, "Understanding the Required Order of Starting and Stopping Components"
- Section 6.2.2.2, "Getting General Information About Starting and Stopping Oracle Fusion Middleware Components"

6.2.2.1 Understanding the Required Order of Starting and Stopping Components

Before you manually start and stop the Oracle Identity Management components after an automated deployment, you must understand the order in which components must be started.

When stopping the Oracle Identity and Access Management environment, stop the components in the following order:

1. Oracle Mobile Security Access Server
2. Oracle HTTP Server
3. Business Intelligence Publisher (BIP) Server
4. Oracle Identity Manager
5. Oracle SOA Suite
6. The Oracle Identity Manager Administration Server
7. Oracle Policy Manager Server
8. Oracle Mobile Security Manager Server (OMSM)
9. Oracle Access Manager
10. The Oracle Access Manager Administration Server
11. Node Manager
12. Oracle Unified Directory (OUD) or Oracle Internet Directory (OID)

When starting the components in an Oracle Identity and Access Management environment, stop the components in this order:

1. Oracle Unified Directory (OUD) or Oracle Internet Directory (OID)
2. Node Manager
3. Oracle Access Manager Administration Server
4. Oracle Access Manager
5. Oracle Mobile Security Manager Server (OMSM)
6. Oracle Policy Manager Server
7. Oracle Identity Manager Administration Server
8. Oracle SOA Suite
9. Oracle Identity Manager
10. Business Intelligence Publisher (BIP) Server
11. Oracle HTTP Server
12. Oracle Mobile Security Access Server

6.2.2.2 Getting General Information About Starting and Stopping Oracle Fusion Middleware Components

For general information on starting and stopping Oracle Fusion Middleware products and components, see "Starting and Stopping Components" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

7

Validating Deployment

The Deployment process includes several validation checks to ensure that everything is working correctly. This chapter describes additional checks that you can perform for additional sanity checking.

This chapter contains the following sections:

- Section 7.1, "Verifying Connectivity to the Administration Server"
- Section 7.2, "Validating the Access Manager and Oracle Mobile Security Manager Configuration"
- Section 7.3, "Validating Oracle Identity Manager"
- Section 7.4, "Validating WebGate and the Access Manager Single Sign-On Setup"

7.1 Verifying Connectivity to the Administration Server

To verify connectivity, refer to one of the sections below based on your topology selection:

- Section 7.1.1, "Verifying the Administration Server Connectivity for Oracle Access Management"
- Section 7.1.2, "Verifying Administration Server Connectivity for Oracle Identity Manager"

7.1.1 Verifying the Administration Server Connectivity for Oracle Access Management

Verify that you can access the administration console, and the Oracle Enterprise Manager Fusion Middleware Control by accessing the URLs shown in Table 7–1. Use the consoles to confirm that all Managed Servers are up and running.

The table also provides information about the user that you must log in as to access these URLs.

In the table, *IAMHOST* represents the fully qualified name of the host where you have automatically installed and configured Oracle Identity Manager with the LCM Tools.

Table 7–1 URL and user information for verifying Oracle Access Management

URL	User
http://*IAMHOST*:7777/console	weblogic_idm
http://*IAMHOST*:7777/em	weblogic_idm
http://*IAMHOST*:7777/oamconsole	oamadmin
http://*IAMHOST*:7777/access	oamadmin

7.1.2 Verifying Administration Server Connectivity for Oracle Identity Manager

Verify that you can access the administration console and the Oracle Enterprise Manager Fusion Middleware Control, using the URLs shown in following tables:

- See Table 7–2 if you are deploying the OIM Only topology.
- See Table 7–3 if you are deploying the OIM, OAM, and OMSS Integrated topology

The tables also provide information about the user that you must log in as to access these URLs.

In both tables, *IAMHOST* represents the fully qualified name of the host where you have automatically installed and configured Oracle Identity Manager with the LCM Tools.

Table 7–2 URL and User Information for Verifying an Oracle Identity Manager Deployment on a Single Host (OIM Only Topology)

URL	User
http://*IAMHOST*:7777/console	weblogic
http://*IAMHOST*:7777/em	weblogic
http://*IAMHOST*:7777/identity	xelsysadm
http://*IAMHOST*:7777/sysadmin	xelsysadm
http://*IAMHOST*:7777/apm	weblogic
http://*IAMHOST*:7777/xmlpserver	bisystemuser

Table 7–3 URL and User Information for Verifying an Oracle Identity Manager Deployment on a Single Host (OIM, OAM, and OMSS Topology)

URL	User
http://*IAMHOST*:7778/console	weblogic_idm
http://*IAMHOST*:7778/em	weblogic_idm
http://*IAMHOST*:7778/identity	xelsysadm
http://*IAMHOST*:7778/sysadmin	xelsysadm
http://*IAMHOST*:7778/apm	weblogic_idm
http://*IAMHOST*:7778/xmlpserver	xelsysadm

7.2 Validating the Access Manager and Oracle Mobile Security Manager Configuration

To validate that Oracle Access Manager and Oracle Mobile Security Manager have been configured correctly, refer to the instructions in "Verifying Oracle Access Manager and Oracle Mobile Security Manager" in the *Installation Guide for Oracle Identity and Access Management*.

7.3 Validating Oracle Identity Manager

To validate that Oracle Identity Manager has been configured correctly, see the instructions in "Verifying the Oracle Identity Manager Installation" in the *Installation Guide for Oracle Identity and Access Management*.

7.4 Validating WebGate and the Access Manager Single Sign-On Setup

To validate that WebGate is functioning correctly, open a web browser and go the OAM console at the following URL:

`http://IAMHOST/oamconsole`

On the Access Manager Login page, enter your OAM administrator user name (for example, `weblogic_idm`) and password. You should see the Access Manager console displayed.

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console at the following URL:

`http://IAMHOST/console`

Or, validate access to Oracle Enterprise Manager Fusion Middleware Control using this URL:

`http://IAMHOST/em`

In either case, the Access Manager Single Sign-On page should display. Provide the credentials for the `weblogic_idm` user to log in.

8

Troubleshooting Oracle Identity and Access Management Deployment

This chapter describes how to troubleshoot common problems that you might encounter when using Oracle Identity and Access Management Deployment tools.

In addition to this chapter, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

This chapter contains the following sections:

- Section 8.1, "Getting Started with Troubleshooting"
- Section 8.2, "Using My Oracle Support for Additional Troubleshooting Information"

8.1 Getting Started with Troubleshooting

This section describes how to use the log files and how to recover from deployment failures. It contains the following topics:

- Section 8.1.1, "Using the Log Files"
- Section 8.1.2, "Recovering From Oracle Identity and Access Management Deployment Failure"

8.1.1 Using the Log Files

If you are performing deployment using the wizard, from any phase screen, click on the icon under the **Log** field to see the logs for the current phase. A new window opens showing the logs. The logs are searchable using the search box at the top of this new window. The log window does not refresh on its own, so click on the refresh button besides the search box at the top of this window to refresh the logs.

To check why a phase failed when the wizard is not running, check the corresponding logs files present under the logs directory:

LCM_STORE/provisioning/logs/*hostname*.

LCM_STORE is the **Lifecycle Management Store Location** directory that you specified on the Installation and Configuration screen when you created the deployment profile. For more information, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

8.1.2 Recovering From Oracle Identity and Access Management Deployment Failure

Oracle Identity and Access Management Deployment has a limited Cleanup and Recovery feature, which you can use if the automated deployment fails.

For more information about cleaning up an environment, see Appendix A, "Cleaning Up an Environment Before Rerunning IAM Deployment".

8.2 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

> **Note:** You can also use My Oracle Support to log a service request.

You can access My Oracle Support at `https://support.oracle.com`.

A

Cleaning Up an Environment Before Rerunning IAM Deployment

When you deploy Oracle Identity and Access Management using the `runIAMDeployment.sh` command, you must complete each stage in the topology before beginning the next stage. If a stage fails, you must clean up and start over. This chapter explains how to perform the Cleanup and Recory task.

This section contains the following topics:

- Section A.1, "About the Cleanup and Restore Feature"
- Section A.2, "Manual Cleanup of Environment"

A.1 About the Cleanup and Restore Feature

If the deployment fails, note the name of teh phase where the failure occurred, and then check the logs to determine a cause.

When you are ready to cleanup and attempt another deployment, do one of the following:

- If the deployment failed in the Preconfigure or Install phases, then use Cleanup and Restore to cleanup the environment so you can start the deployment again from the beginning.
- If deployment fails between the Preconfigure stage and the Validate stage, then use the Cleanup and Restore feature to clean up the environment and restore it back to the post-install stage.

For example, if the deployment fails during the postconfigure stage, you can use Cleanup and Restore to clean up any changes made since you successfully completed the install stage.

Cleanup and Restore can be performed using either the command line deployment tool or the Deployment wizard.

A.1.1 Directories Affected by Cleanup and Restore

When you use Cleanup and Restore, it removes the following directories from the Lifecycle Management Store Location (*`LCM_STORE`*) directory:

- `lcmconfig`
- `provisioning`
- `internal`
- `keystores`

In addition, the feature removes all content from the shared configuration (*IDMTOP*/config) directory, except the provisioning directory. The provisioning directory is required by the Cleanup and Restore feature.

A.1.2 Where Does Cleanup and Restore Save Its Data?

When you successfully completed the install stage, a backup file restore.zip is created inside the IDMLCM_HOME directory. Cleanup and Restore uses this file to restore the deleted directories during the Restore operation.

A.1.3 About Managing Schemas When You Use Cleanup and Restore

If you created the required schemas in the database using the Automated Installer, then Cleanup and Restore automatically drops and recreates the product schemas.

If you created the schemas manually with the Repository Creation Utility (RCU), then you must use RCU to drop and recreate the schemas manually.

Additionally, if you created the schemas manually and you are deploying the integrated OIM, OAM, and OMSS topology, then you must run RCU twice to drop the schemas you created for the OIM domain and then a second time to drop the schemas you created for the OAM domain.

A.1.4 Performing Cleanup and Restore Using the Command Line Deployment Tool

This section provides information about performing Cleanup and Restore using the command line deployment tool.

If the failure occurred in the Preconfigure or Install phase, then run the Cleanup and Restore command line once to cleanup the envirnoment, so you attempt the deployment again from the beginning.

If the failure occurred in after the Install phase, then you must execute two commands, first the Cleanup command, and then the Restore command. The Restore command will restore the environment to its post-install phase state.

A.1.4.1 Using the Command Line to Clean Up a Failed Deployment

The command syntax for performing cleanup is as follows:

```
IDMLCM_HOME/runIAMDeployment.sh -responseFile response_file_name -target
cleanup-failed_phase_name
```

In this example:

- Replace *IDMLCM_HOME* with the full path the LCM Tool Oracle home, which was created when you installed the LCM Tools.

  For more information, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

- Replace *response_file* with the complete path to the location of the deployment response file.

  You specified the response file name and directory on the **Summary** screen when you ran the wizard to create the deployment response file.

- Replace *failed_phase_name* with the name of the phase that failed in the previous deployment session.

Use the following examples as a guide when cleaning up the environment with Cleanup and Restore:

```
runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-preconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-configure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-configure-secondary

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-postconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-startup

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target cleanup-validate
```

A.1.4.2 Using the Command Line to Restore the Install Phase Content

The command syntax for performing a restore is as follows:

```
IDMLCM_HOME/runIAMDeployment.sh -responseFile response_file_name -target
restore-failed-phase_name
```

In this example:

- Replace *IDMLCM_HOME* with the full path the LCM Tool Oracle home, which was created when you installed the LCM Tools.

  For more information, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

- Replace *response_file* with the complete path to the location of the deployment response file.

  You specified the response file name and directory on the **Summary** screen when you ran the wizard to create the deployment response file.

- Replace *failed-phase_name* with the name of the phase that failed in the previous deployment session.

Use the following examples as a guide when restoring the environment with Cleanup and Restore:

```
runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-preconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-configure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-configure-secondary

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-postconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-startup

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target restore-validate
```

A.1.5 Performing Cleanup and Restore Using the Identity and Access Management Deployment Wizard

When using the Identity and Access Management Deployment wizard, the Cleanup and Restore button becomes available whenever any of the provisioning phase fails.

To perform Cleanup and Restore using the Identity and Access Management Deployment wizard:

1. Click **Cleanup and Restore**.

   Cleanup and Restore dialog window that displays the current progress of cleanup and restore process appears.

2. After Cleanup and Restore is performed successfully, read the message on the pop up dialog and close the Cleanup and Restore window by clicking **OK**.

A.2 Manual Cleanup of Environment

If cleanup and restore operation fails for any reason, or if you want to clean up a deployed environment manually before starting another cycle of deployment, proceed as follows:

1. On your host, stop all Identity and Access Management processes, services and servers.

   If you have successfully completed the Preconfigure and Configure deployment phases, then you can use the start and stop scripts provided by the LCM Tools. For more information, see Section 6.2, "Starting and Stopping Oracle Identity and Access Management Components After an Automated Deployment".

   If you have not successfully completed the Preconfigure and Configure deployment phases, then one way to ensure all processes and servers are stopped is to reboot the host computer.

2. On your host, remove the contents of the shared configuration directory (for example, *IDMTOP*/config).

3. Remove the contents of the directories *LCM_STORE* and *IDMTOP*.

   LCM_STORE is the **Lifecycle Management Store Location** directory and *IDMTOP* is the **Software Installation Location** directory you specified on the Select Installation and Configuration Locations screen.

   For more information, see Section 2.5, "About the Deployment Repository and LCM Tools Directory Structure".

4. Drop the database schema using RCU.

   If you are using Oracle Internet Diretory (OID), then ensure that you select the ODS schema, which is not selected by default. Oracle Identity and Access Management deployment will fail during the next run if you don't perform this step correctly.

After you have performed these steps, you can attempt another deployment using the LCM Tools.