Oracle® Fusion Middleware

Deployment Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E48635-04

October 2014

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 (11.1.2.2.0)

E48635-04

Primary Author: Rajesh Gouthaman

Contributors: Jatan Rajvanshi, Kopal Sinha, Anupama Pundpal, Michael Rhys, Ellen Desmond, Gururaj BS, Sandeep Reddy Vinta, Javed Beg, Warren Zheng, Mehul Poladia, Jeremy Banford, Nagasravani Akula

Contents

5 Performing Oracle Identity and Access Management Deployment

6 Post Deployment Tasks

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 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 Release 11.1.2.2 documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.*
- *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*
- *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Solaris Operating System*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for HP-UX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for hp Tru64 UNIX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for AIX Based Systems*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*
- *Oracle Database Backup and Recovery User's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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

Introduction and Preparation

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:

1

Introduction to Identity and Access Management Deployment

This chapter provides an introduction to Oracle Identity and Access Management Deployment.

This chapter also describes and illustrates the deployment reference topologies employed in this guide.

The Oracle Identity and Access Management Deployment Wizard and related lifecycle tools were developed to automate Oracle Identity and Access Management Deployment and reduce the time required to install and configure Oracle Identity and Access Management components.

Note: This guide describes how to install Oracle Identity and Access Management with High Availability (HA) in two scenarios, such as the following:

- Oracle Identity Manager (OIM) Only
- Oracle Access Management Suite Only.

The key to a successful deployment is planning and preparation. The road map for installation and configuration at the end of this chapter directs you to the appropriate chapters for the tasks you need to perform. Use this chapter to help you map the examples used in this guide to your own deployment.

This chapter contains the following sections:

1.1 Planning Your Deployment

A deployment for Oracle Identity and Access Management consists of the following parts:

- A database for storing policy information and information specific to the identity and access management components being deployed.

- Identity and Access Management components can be divided into three categories:
  - Directory Services: one or more highly available directories for storing identity information
  - Identity Management Provisioning: Oracle Identity Manager
  - Access Control: Oracle Access Management Access Manager
- A highly available web tier which is used to access Identity and Access Management components.
- A highly available load balancer, which is used to distribute load between the web servers. The load balancer is also used to off load SSL encryption to ensure that communication between user sessions and Oracle Identity and Access Management are encrypted, but without the overhead of having to enable SSL between the individual Identity and Access Management components.

This guide explains in detail how to deploy two topologies supported in this early release of Oracle Identity and Access Management (11.1.2.2). This topology is not the only one supported by Oracle, but it is deemed to be the most common.

1.2 Understanding Oracle Identity and Access Management Deployment Topologies

Each topology is divided into tiers for increased security and protection. The tiers are separated by firewalls that control access from one tier to the next. The goal is to prevent unauthorized traffic. In an Internet-facing topology, for instance, it should not be possible to directly access a database from the Internet zone. Only applications deployed in the application zone should have access to the database.

The diagram shows three tiers:

- Web Tier
- Application Tier
- 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 alongside the database tier. Note that the common practice is to use an existing directory on the network.

This section contains the following topics:

- Section 1.2.1, "About the Web Tier"
- Section 1.2.2, "About the Application Tier"
- Section 1.2.3, "About the Database Tier,"

1.2.1 About the Web Tier

The web tier is in the DMZ Public Zone. The HTTP Servers are deployed in the web tier.

Most of the Identity and Access Management components can function without the web tier, but to properly support high availability and SSO between IAM components out of the box, the web tier is required. All topologies created using the Deployment Tool come with a configured web tier.

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Access Manager component), and the `mod_wl_ohs` plug-in module 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.
- In the OAM-Only deployment scenario, WebGate in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on OAMHOST1 and OAMHOST2, in the Identity Management zone. WebGate and Access Manager are used to perform operations such as user authentication.

On the firewall protecting the web tier, the HTTP ports are 443 (*HTTP_SSL_PORT*) for HTTPS and 80 (*HTTP_PORT*) for HTTP.

1.2.1.1 High Availability Provisions

If the Oracle HTTP server fails on the WEBHOST1, Oracle Process Management and Notification (OPMN) server attempts to restart it.

1.2.1.2 Security Provisions

The Oracle HTTP Servers process requests received using the URLs `igdadmin.mycompany.com`, `sso.mycompany.com`, and `iadadmin.mycompany.com`. The names `igdadmin.mycompany.com`, `sso.mycompany.com`, and `iadadmin.mycompany.com` are only resolvable inside the firewall. This prevents access to sensitive resources such as the Oracle WebLogic Server console and Oracle Enterprise Manager Fusion Middleware Control console from the public domain.

1.2.2 About the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Manager, Oracle Access Manager and Oracle Enterprise Manager Fusion Middleware Control are the key Java EE components that are deployed in this tier. Applications in this tier benefit from the High Availability support of Oracle WebLogic Server.

If a directory tier exists in the deployment topology, the Identity and Access Management applications in the application tier interact with the directory tier as follows:

- They leverage the directory tier for enterprise identity information.
- In some cases, they leverage the directory tier (and sometimes the database in the data tier) for application metadata.
- Oracle Enterprise Manager Fusion Middleware Control is an administration tool that provides administrative functionalities to the components in the application tier as well as the directory tier.
- WebLogic Server has built-in web server support. If enabled, the HTTP listener exists in the application tier as well.

The application tier includes the following components:

- Oracle Access Management Suite. However, only Oracle Access Manager (OAM) is configured and activated by the Identity and Access Management Deployment Wizard. (OAM). If necessary, other components of the Oracle Access Management Suite, such as Oracle Identity Federation and Secure Token Service, can be configured manually.

- The governance components, which are Oracle Identity Manager (OIM) and Oracle SOA Suite (SOA).
- The administrative components of Identity and Access Management, including Oracle Identity Manager, which is used for user provisioning. These servers also run Oracle SOA, which is used exclusively by Oracle Identity Manager.

In addition:

- OAMHOST1 hosts an Oracle WebLogic Administration Server for **IAMAccessDomain**. Inside the administration server are managerial and navigational components for the domain including: Oracle WebLogic Console, Oracle Enterprise Manager Fusion Middleware Control, and Access Manager Console.
- OIMHOST1 hosts an Oracle WebLogic Administration Server for **IAMGovernanceDomain**. Inside the administration server are managerial and navigational components for the domain including: Oracle WebLogic Console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Authorization Policy Manager.
- The WebLogic Administration server is a singleton process. That is, it can only be started on one server at a time. In the event that the host running the administration server fails, the Administration server can be manually started on a different host.

1.2.2.1 About WebLogic Domains

A domain is the basic administration unit for WebLogic Server instances. A domain consists of one or more WebLogic Server instances (and their associated resources) that you manage with a single Administration Server. You can define multiple domains based on different system administrators' responsibilities, application boundaries, or geographical locations of servers.

In the topology used in this version of the guide, products are deployed to two separate Middleware Home directories and to two separate WebLogic domains:

- **IAMAccessDomain** - Hosts Oracle Access Management suite components.
- **IAMGovernanceDomain** - Hosts Oracle Identity Manager, SOA, and other governance components.

1.2.2.2 Security Provisions

Oracle WebLogic Server Console, Oracle Enterprise Manager Fusion Middleware Control console, and Oracle Access Management Console are only accessible through a virtual host configured on the load balancer, which is only available inside the firewall.

1.2.3 About the Database Tier

Starting with 11g Release 2 (11.1.2), policy information is stored in the database. The database is also used for storing information specific to the Identity and Access Management components being deployed.

In some cases, the directory tier and database tier might be managed by the same group of administrators. In many enterprises, however, database administrators own the data tier while directory administrators own the directory tier.

1.3 Products Deployed Using the Oracle Identity and Access Management Deployment Wizard

The following products can be installed, configured, and integrated using the Oracle Identity and Access Management Deployment Wizard:

- Oracle WebLogic Server
- Oracle SOA Suite (required for Oracle Identity Manager only)
- Oracle Identity Manager
- Oracle Access Management
- Oracle Unified Directory
- Oracle HTTP Server
- Webgate

The products that are installed and configured depend on the option that you select on the **Select IAM Products** screen of the Oracle Identity and Access Management Deployment Wizard, when you create the deployment response file. For more information, see Section 4.4.1.6, "Select IAM Products"

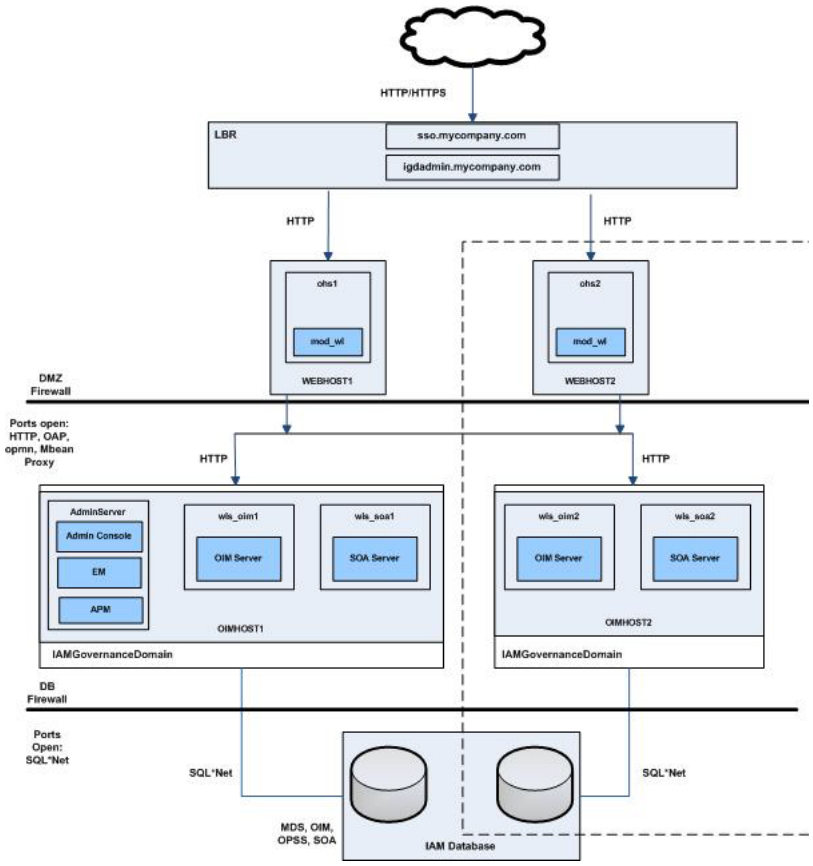
1.4 Reference Topologies Documented in This Version of the Guide

In this version of the Identity and Access Management deployment guide, the following reference HA topologies are documented:

- Only Oracle Identity Manager in an HA Environment
- Only Oracle Access Management in an HA Environment

1.4.1 Only Oracle Identity Manager in an HA Environment

This section illustrates and describes the Oracle Identity Manager Only (OIM-Only) installation scenario.



Oracle Identity Governance/Manager empowers user self-service, simplifies account administration, and streamlines audit tasks resulting in a lower overall total cost of ownership for managing identities. The Oracle Identity Manager Only (OIM-Only) topology diagram includes icons and symbols that represent the hardware load balancer, host computers, firewalls, and other elements of the topology. At a high level, it shows the main components of the topology, including the following:

- The Load Balancer: The load balancer can be configured to receive user requests on either Port 80 (HTTP) and Port 443 (HTTPS). If HTTPS is chosen, SSL is terminated (where appropriate), and the request are passed onto the Oracle HTTP servers using Port 7777.
- The Web Tier: Each host in the web tier hosts an Oracle HTTP Server instance and the mod_wl_ohs module.
- The Application Tier: There are two hosts, OIMHOST1 and OIMHOST2. A single WebLogic administration domain, IAMGovernanceDomain, spans these hosts. Managed Servers run on both OIMHOST1 and OIMHOST2 in a WebLogic clustered setup. For example, `wls_oim1` and `wls_soa1` run on OIMHOST1. Similarly, wls_oim2 and wls_soa2 run on OIMHOST2. Requests are received from the Web Tier. Each host contains Managed Servers for the following products:
  - Oracle Identity Manager (OIM)
  - SOA that hosts a SOA Server and corresponding JRF/OPSS processes (exclusively used by Oracle Identity Manager)

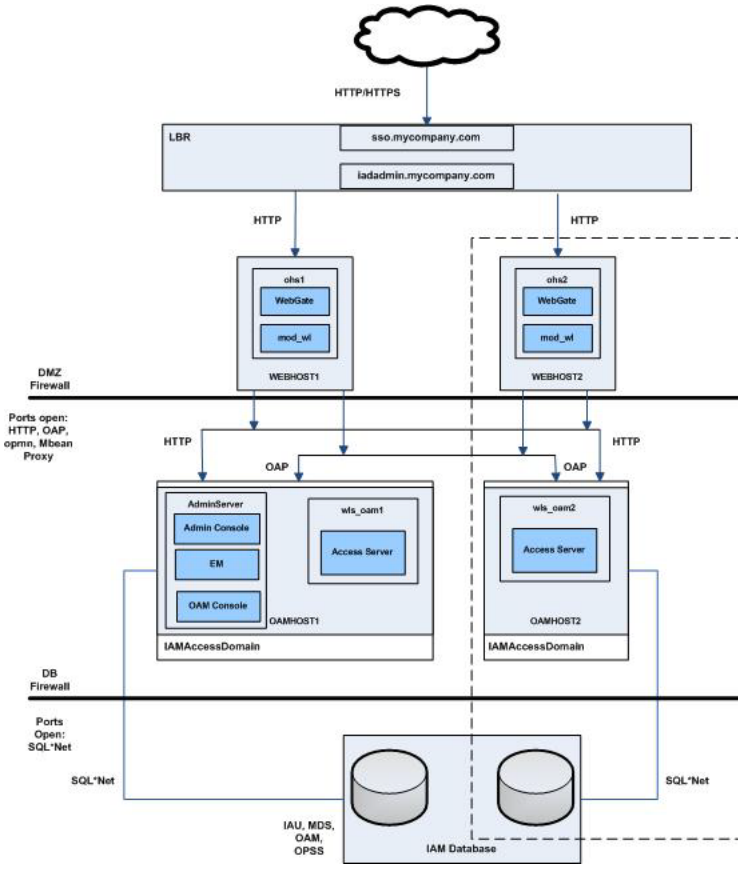
  OIMHOST1 also contains the WebLogic Administration Server, which hosts the WebLogic Console, Enterprise Manager Fusion Middleware Control, and Authorization Policy Manager (APM). Oracle Identity Manager Administration

Console (/sysadmin) and SOA Console are hosted on the OIM Managed Server. In the event of the failure of OIMHOST1, the WebLogic Administration Server can be started on OIMHOST2 manually.

- Firewalls: These are used to separate the Web, Application, and Database tiers into different zones. WEBHOST1 and WEBHOST2 reside in the DMZ.

1.4.2 Only Oracle Access Management in an HA Environment

This section illustrates and describes the Oracle Access Management Only (OAM-Only) installation scenario.



Oracle Access Management suite gives customers the flexibility to deploy a comprehensive solution delivering authentication, single sign-on, authorization, mobile and social sign-on, identity propagation, and risk-based authentication and authorization at the network perimeter.

Oracle Access Manager (OAM) enables your users to seamlessly gain access to web applications and other IT resources across your enterprise. It provides a centralized and automated single sign-on (SSO) solution, which includes an extensible set of authentication methods and the ability to define workflows around them. It also contains an authorization engine, which grants or denies access to particular resources based on properties of the user requesting access as well as based on the environment from which the request is made. Comprehensive policy management, auditing, and integration with other components of your IT infrastructure enrich this core functionality.

This topology will not service federated requests out of the box.

The topology diagram includes icons and symbols that represent the hardware load balancer, host computers, firewalls, and other elements of the topology. At a high level, it shows the main components of the topology, including the following:

- The Load Balancer: The load balancer receives user requests on Port 80 (HTTP) and Port 443 (HTTPS), strips out the SSL (where appropriate) and passes the requests onto the Oracle HTTP servers using Port 7777.
- The Web Tier: Each host in the web tier hosts an Oracle HTTP Server instance and the mod_wl_ohs module.
- The Application Tier: There are two hosts, OAMHOST1 and OAMHOST2. A single WebLogic administration domain, `IAMAccessDomain`, spans these hosts. Managed Servers run on both OAMHOST1 and OAMHOST2 in a WebLogic clustered setup. For example, `wls_oam1` runs on OAMHOST1. Similarly, `wls_oam2` runs on OAMHOST2. Requests are received from the Web Tier. Each host contains Managed Servers for Oracle Access Manager.

  OAMHOST1 also contains the WebLogic Administration Server, which hosts the WebLogic Console, Enterprise Manager Fusion Middleware Control, and Oracle Access Manager Administration Console. In the event of the failure of OAMHOST1, the WebLogic Administration Server can be started on OAMHOST2 manually.
- Firewalls: These are used to separate the Web, Application, and Database tiers into different zones. WEBHOST1 and WEBHOST2 reside in the DMZ.

Note: When you configure Oracle Access Management using the Oracle Identity and Access Management Deployment Wizard, only Oracle Access Manager is enabled, by default. For enabling other services including Security Token Service, Identity Federation, and Oracle Access Management Mobile and Social, refer to "Enabling or Disabling Available Services" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

2

Preparing for Oracle Identity and Access Management Deployment

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:

2.1 Hardware Requirements for Oracle Identity and Access Management Deployment

You can deploy either a distributed or a consolidated topology. The consolidated topology uses a small number of powerful servers, which makes the deployment simpler. It is, however, not mandatory to use such powerful servers. The distributed topology uses a larger number of smaller servers.

For detailed hardware requirements, see *Oracle Fusion Middleware System Requirements and Specifications*.

Note: Oracle recommends configuring all nodes in the topology identically with respect to operating system levels, patch levels, user accounts, and user groups.

2.2 Software Requirements for Oracle Identity and Access Management Deployment

This section describes the software required for an Oracle Identity and Access Management deployment.

This section contains the following topics:

- Section 2.2.1, "Software Versions"
- Section 2.2.2, "About Obtaining Software"
- Section 2.2.3, "Summary of Oracle Homes"
- Section 2.2.4, "Applying Patches and Workarounds"

2.2.1 Software Versions

Table 2–1, " Software Versions Used" lists the Oracle software you need to obtain before starting the procedures in this guide.

Table 2–1 Software Versions Used

Short Name	Product	Version
OHS11G	Oracle HTTP Server	11.1.1.7.0
JRockit	Oracle JRockit	jrockit-jdk1.6.0_29-R28.2.0-4.0.1 or newer
WLS	Oracle WebLogic Server	10.3.6.0
IAM	Oracle Identity and Access Management	11.1.2.2.0
SOA	Oracle SOA Suite	11.1.1.7.0
WebGate	WebGate 11*g*	11.1.2.2.0
RCU	Repository Creation Utility	11.1.2.2.0

2.2.2 About Obtaining Software

You must download the Identity and Access Management deployment repository, not the individual components. The Identity and Access Management deployment repository contains all the installers required to deploy a new Oracle Identity and Access Management environment.

This repository is referred to as *REPOS_HOME* in this guide.

For complete information about downloading Oracle Fusion Middleware software, see the *Oracle Fusion Middleware Download, Installation, and Configuration Readme* for this release, at: http://docs.oracle.com/cd/E23104_01/download_readme.htm

2.2.3 Summary of Oracle Homes

Oracle binaries are installed into an Oracle Fusion Middleware home. Individual products are installed into Oracle homes within the Middleware home. Table 2–2 is a summary of the Middleware homes and Oracle homes used in this document.

The installation and configuration of Oracle Identity Management is outside the scope of this Guide. See *Oracle Fusion Middleware High Availability Guide* for more information.

Table 2–2 Summary of Homes

Home Name	Home Description	Products Installed
MW_HOME	Consists of the Oracle WebLogic Server home and, optionally, one or more Oracle homes. In the OIM-Only deployment scenario, MW_HOME contains an Oracle Home for Identity and Access Management. WEB_MW_HOME contains an Oracle Home for Oracle HTTP Server. In the OAM-Only deployment scenario, MW_HOME contains an Oracle Home for Identity and Access Management. WEB_MW_HOME contains an Oracle Home for Oracle HTTP Server. Note that each MW_HOME also contains Oracle Common.	
WL_HOME	This is the root directory in which Oracle WebLogic Server is installed. The WL_HOME directory is a peer of Oracle home directory and resides within the *MW_HOME*. Note that WL_HOME is also present separately in the MW_HOME for Identity and Access Management.	Oracle WebLogic Server
IGD_ORACLE_HOME	Each Identity and Access Management MW_HOME contains an Oracle Home for Identity Management. In the OIM-Only deployment scenario, an Oracle Home for Oracle Identity Manager is included. The binary and library files required for Oracle Identity Manager are located in *IAM_MW_HOME*/iam.	Access Manager Oracle Identity Management
IAD_ORACLE_HOME	Each Identity and Access Management MW_HOME contains an Oracle Home for Identity Management. In the OAM-Only deployment scenario, an Oracle Home for Oracle Access Management Suite is included. The binary and library files required for Oracle Access Management are located in *IAM_MW_HOME*/iam.	Access Manager Oracle Identity Management
WEB_ORACLE_HOME	Contains the binary and library files required for Oracle HTTP Server. It is located in *WEB_MW_HOME*/ohs.	Oracle WebGate
SOA_ORACLE_HOME	Contains the binary and library files required for the Oracle SOA Suite. It is located in *IAM_MW_HOME*/soa.	Oracle SOA Suite
ORACLE_COMMON_HOME	Contains the generic Oracle home files. This Oracle home is created automatically by any product installation and is located in *MW_HOME*/oracle_common.	Generic commands
IDMLCM_HOME	A subdirectory of the Oracle Middleware Home directory where the Identity and Access Management Lifecycle Tools will be installed	Identity and Access Management Lifecycle Tools

2.2.4 Applying Patches and Workarounds

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. The deployment tool can apply these patches automatically at the time it runs.

Patches are available for download from `http://support.oracle.com`. You can find instructions for deploying each patch in the enclosed `README.html` file. Download the patches and unzip each patch to the directory appropriate for the product, as listed in Table 2–3. If the directory does not exist, create it.

After unzipping the patch, ensure 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 ensure 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 ensure that the individual patches appear in the correct Patch Directory as listed below.

Table 2–3 Product Patch Directories

Product	Patch Directory
Oracle Common	*REPOS_HOME*/installers/oracle_common/patch
Directory	*REPOS_HOME*/installers/oud/patch/oud
	REPOS_HOME/installers/oud/patch/odsm
Oracle Access Management Access Manager	*REPOS_HOME*/installers/iamsuite/patch/oam
OHS	*REPOS_HOME*/installers/webtier/patch
WebGate	*REPOS_HOME*/installers/webgate/patch
Oracle Identity Manager	*REPOS_HOME*/installers/iamsuite/patch/oim
SOA	*REPOS_HOME*/installers/soa/patch
WebLogic Server	*REPOS_HOME*/installers/weblogic/patch

2.2.4.1 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*.

2.3 Verifying Java

Ensure that your Deployment Repository contains Java. It should reside in a directory called `jdk6`.

2.4 Installing the Database

For information on Database requirements, see Section 3.4, "Overview of Database Preparation".

2.5 Preparing the Database for Repository Creation Utility (RCU)

To prepare the Oracle Database for RCU, follow the instructions in the section "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications*.

2.6 Running Oracle Identity and Access Management Repository Creation Utility (Oracle Identity and Access Management RCU)

Use the Oracle Identity and Access Management version of RCU, which is in the following directory:

REPOS_HOME`/installers/fmw_rcu/linux/rcuHome.zip`

where *REPOS_HOME* is the Oracle Identity and Access Management deployment repository that contains all the installers required to deploy a new Oracle Identity and Access 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
```

You must create and load the appropriate Oracle Identity and Access Management schemas in the database using RCU, before deploying the following Oracle Identity and Access Management components:

- Oracle Identity Manager
- Oracle Access Management

Select the appropriate components from the following table for the topology you are using:

Product	RCU Option	Comments
Oracle Platform Security Services for IAMAccessDomain	AS Common Schemas–Oracle Platform Security Service	Required to hold policy store information.
Oracle Access Management Access Manager	Oracle Access Manager	Audit Services will also be selected.

Product	RCU Option	Comments
Oracle Adaptive Access Manager	Oracle Adaptive Access Manager	This is optional.
Oracle Platform Security Services for IAMGovernanceDomain	AS Common Schemas–Oracle Platform Security Service	Required to hold policy store information.
Oracle Identity Manager	Identity Management–Oracle Identity Manager	Metadata Services, SOA infrastructure, and User Messaging will also be selected.

You must select a single password for all the schema while running the RCU.

For more information about RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Important Notes

- Oracle Identity and Access Management deployment supports separate OIM and OAM databases. If databases are separate for OIM and OAM, then you can provide separate schema prefix and password for OIM and OAM schemas.
- If you are using separate databases, then the Oracle Platform Security Services (OPSS) schema that is used for the policy store, depends on the option that you select on the **Select IAM Products** screen of the Oracle Identity and Access Management Deployment Wizard. This screen appears when you create the deployment response file. For more information, see Section 4.4.1.6, "Select IAM Products".
  - **Oracle Identity Manager (OIM) Only**: If you select this option, then the Oracle Platform Security Services (OPSS) schema in the OIM database is used.
  - **Oracle Access Manager (OAM) Suite Only**: If you select this option, then the Oracle Platform Security Services (OPSS) schema in the OAM database is used.
  - **OIM-OAM Integrated and Oracle Unified Directory (OUD)**: If you select this option, then you must create two Oracle Platform Security Services (OPSS) schemas; one for OIM in the OIM database, and one for OAM in the OAM database.

    Note: The **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option is not documented in this guide. For information about this deployment option, refer to *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

- 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".
- You must create different schema prefix, host, port, and servicename for OIM, and OAM schemas. However, the schema prefix, host, port, servicename, and password should be the same for OIM and all OIM dependent components. Similarly, the schema prefix, host, port, servicename, and password should be the same for OAM and all OAM dependent components.

2.7 About the Lifecycle Management and Deployment Repository

The lifecycle repository contains the Lifecycle Management Tools, such as the deployment and patching tools. It also contains a software repository which includes the software to be installed as well as any patches to be applied.

> **Note:** It is important that minimum privileges are assigned to UNIX users on the Deployment Repository. In order to do this, navigate to the extracted IAM Deployment Repository, and run the following command. This updates the permissions on the content of the repository.
>
> ```
> chmod ¿R 755 *
> ```

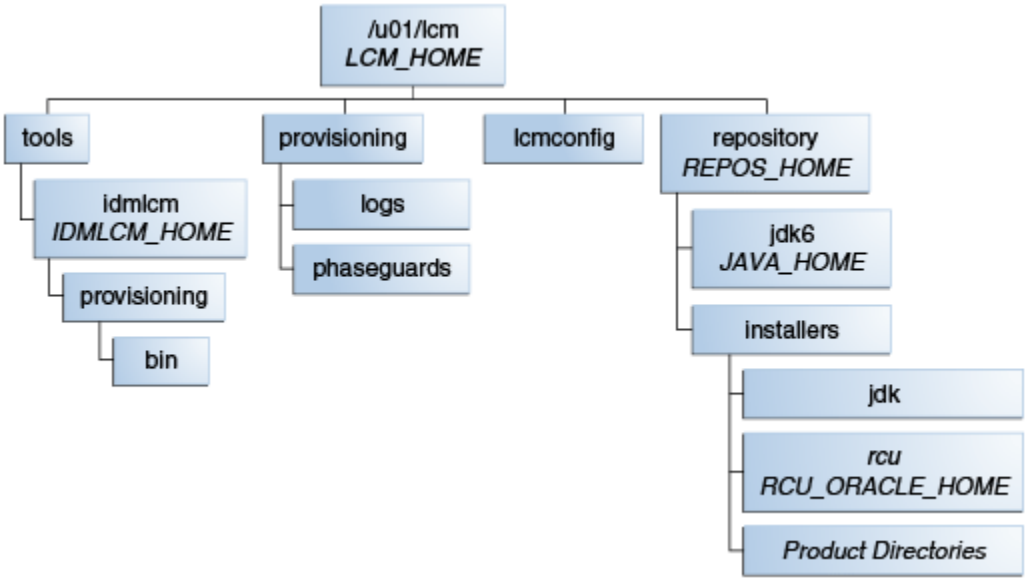
You need a separate share to hold the Lifecycle Management Tools and Deployment Repository. This share is only required during deployment and any subsequent patching. After deployment is complete, you can unmount this share from each host.

> **Note:** If you have patches that you want to deploy using the patch management tool, you must remount this share while you are applying the patches.

Ideally, you should mount this share on ALL hosts for the duration of deployment. Doing so will make the deployment process simpler, as you will not need to manually copy any files, such as the keystores required by the Web Tier.

If your organization prohibits sharing the `LCM_HOME` to the webtier hosts (even for the duration of deployment), you must create a local copy of the contents of this share on the DMZ hosts and make manual file copies during the deployment phases. For more information, refer to Section 5.3, "Deploying Identity and Access Management Without a Common LCM_HOME".

Figure 2–1 Deployment Repository Structure



2.7.1 More Information About Shared and Local Storage

For information about the shared storage structure, refer to the "Shared Storage" topic in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

For information about the local storage structure, refer to the "Private Storage" topic in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Note: Based on your topology selection, some components mentioned in the above sections of *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* may not be applicable to your deployment scenario.

2.8 Installing the Oracle Identity and Access Management Lifecycle Tools

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

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

REPOS_HOME/installers/idmlcm/idmlcm/Disk1

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

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

On UNIX:

```
cd REPOS_HOME/installers/idmlcm/idmlcm/Disk1
./runInstaller -jreLoc REPOS_HOME/jdk6
```

Then proceed as follows:

1. On the Welcome page, click **Next**.
2. If you are using a UNIX platform, and you have not previously installed an Oracle product on this host, you might be presented with the Specify Inventory Directory page, which prompts you for the location of the **Inventory Directory**. This directory is used to keep track of all Oracle products installed on this host. If you see this page, proceed as follows:

   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. Click **OK** to continue.

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

If you do not have root access on this host but want to continue with the deployment, select **Continue installation with local inventory**.

Click **OK** to continue.

3. On the Prerequisite Checks page, verify that checks complete successfully, then click **Next**.
4. On the Specify Install Location page, enter the following information:
   a. **Oracle Middleware Home** - This is the parent directory of the directory where the Identity and Access Management Lifecycle Tools will be installed.
   b. **Oracle Home Directory** - This is a subdirectory of the Oracle Middleware Home directory where the wizard will be installed. For example:

      `idmlcm`

      In the current guide, this subdirectory is referred to as *`IDMLCM_HOME`*.

   Click **Next**.
5. On the Installation Summary page, click **Install**.
6. On the Installation Progress page, click **Next**.
7. On the Installation Complete page, click **Finish**.

3

Preparing the Environment for Identity and Access Management Deployment on Multiple Hosts

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

This preparation includes network, storage, servers, and database.

This chapter includes the following topics:

3.1 Overview of Network Preparation

You must configure several virtual servers and associated ports on the load balancer for different types of network traffic and monitoring. These virtual servers should be configured to the appropriate real hosts and ports for the services running. Also, the load balancer should be configured to monitor the real host and ports for availability so that the traffic to these is stopped as soon as possible when a service is down. This ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

3.1.1 More Information About Network Preparation

For more information about preparing your network, see the "Preparing the Network for an Enterprise Deployment" chapter in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

The Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management describes the following topics:

- Virtual server names used by the topology

Note: For Oracle Identity Manager (OIM) Only HA deployment, you require VIPs for the Administration Server, `wls_oim1`, `wls_oim2`, `wls_soa1`, and `wls_soa2`.

For Oracle Access Manager (OAM) Suite Only HA deployment, you require VIP for the Administration Server only.

- Load balancer configuration
- IP address and virtual IP address requirements
- Firewalls and ports
- Management of Oracle Access Manager communication protocol

3.2 Overview of Storage Preparation

It is important to set up your storage in a way that makes Identity and Access Management deployment easier to understand, configure, and manage. Oracle recommends that you set up your file system according to information provided in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

3.2.1 More Information About Storage Preparation

For more information about preparing the file system, see the "Preparing Storage for an Enterprise Deployment" chapter in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Use the recommendations as a reference to help understand the directory variables used in the installation and configuration procedures. Other directory layouts are possible and supported, but the model adopted in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* is chosen for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery.

The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* describes the following topics:

- Terminology for directories and directory variables
- Recommendations for Binary (Middleware Home) Directories
- Recommended locations for the different directories

3.3 Overview of Server Preparation

Before you deploy Oracle Fusion Middleware on new hardware, you must set up the servers you plan to use so that the Oracle Software can work in an optimum fashion. Specifically, you must ensure that:

- The servers are running a certified operating system with the required software patches installed.
- You have configured the UNIX Kernel correctly.
- You have created Users and Groups to own the Oracle software.

3.3.1 More Information About Server Preparation

For more information about preparing the servers, see the "Configuring the Servers for an Enterprise Deployment" chapter in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Use the settings described in the above document as only a guide. After using your Oracle software, you should use operating system utilities to tune the configuration to ensure that you are maximizing the potential of your servers.

The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* describes the following topics:

- Verifying server and operating System
- Meeting hardware and software requirements
- Meeting operating system requirements
- Enabling unicode support
- Enabling virtual IP addresses (optional)
- Mounting shared storage onto the host
- Configuring users and groups

3.4 Overview of Database Preparation

The Identity and Access Management components in the deployment use database repositories.

You must complete the following steps:

1. Verify the database requirements, as described in "Verifying the Database Requirements for an Enterprise Deployment" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.
2. Install and configure the Oracle database repositories, as described in "Installing the Database for an Enterprise Deployment" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.
3. Create database services, as described in "Creating Database Services" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.
4. Ensure that you have prepared your database for running the Repository Creation Utility (RCU), as described in Section 2.5, "Preparing the Database for Repository Creation Utility (RCU)".
5. Ensure that you have created the required Identity and Access Management schemas in the database using the Repository Creation Utility (RCU), as described in Section 2.6, "Running Oracle Identity and Access Management Repository Creation Utility (Oracle Identity and Access Management RCU)".

   For information on creating Identity and Access Management schemas in an Oracle RAC Database, refer to the "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU" topic in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

3.4.1 Backing up the Database

Whenever you add a new component to the configuration, you must back up the database, as described in "Backing Up the Database" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Perform this backup after creating domains or adding components such as Oracle Access Management or Oracle Identity Manager.

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:

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:

4.1 Overview of Deployment Response File

Before you can perform deployment, you must provide information about your topology to the Oracle Identity and Access Management Deployment Wizard. Once you have provided all the necessary input, the wizard will create a deployment response file that you use to perform the 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 Identity and Access Management Deployment Wizard

Before running the Oracle Identity and Access Management Deployment Wizard, ensure that the environment variable `JAVA_HOME` is set to *`REPOS_HOME`*`/jdk6`

To start the Oracle Identity and Access Management Deployment Wizard, go to the following directory:

`IDMLCM_HOME``/provisioning/bin`

where *`IDMLCM_HOME`* is the directory where you installed the Oracle Home Directory for Oracle Identity and Access Management, using the installation script for the Oracle Identity and Access Management Deployment Wizard and Oracle Identity and Access Management Patching Tools, as described in Section 2.8, "Installing the Oracle Identity and Access Management Lifecycle Tools."

On Linux or UNIX, run the following command:

```
./iamDeploymentWizard.sh
```

After the Oracle Identity and Access Management Deployment Wizard starts, proceed to one of the following section based on your topology selection:

4.3 Creating a Deployment Response File for a Single-Host Topology

Complete the following steps to create a new Deployment Response File for a single-host 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. Start the Deployment Wizard by performing the steps in Section 4.2, "Starting the Identity and Access Management Deployment Wizard". After you complete those steps, the Welcome screen appears.

   Use the Welcome screen to learn more about the wizard, including some prerequisites for using it. The Welcome screen provides a brief overview of the wizard and lists some requirements that must be met.

   Click **Next** on the Welcome screen.

2. If you are presented with the Specify Inventory Directory screen, proceed as described in Step 2 in Section 2.8, "Installing the Oracle Identity and Access Management Lifecycle Tools." Click **OK** to continue. The Choose IAM Installation Options screen appears.

3. On the Choose IAM Installation Options screen, select **Create a New Identity and Access Management Environment Deployment Response File** if you are creating a response file for the first time. Click **Next**. The Specify Security Updates screen appears.

4. 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 email 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.

   Click **Next**. The Describe Response File screen appears.

5. On the Describe Response File screen, specify descriptive information to identify the response file. The information entered on this screen is metadata information. This information can be used to uniquely identify a response file if multiple response files are created.

   - **Response File Title**: The Oracle Identity and Access Management Deployment Wizard provides the default title `Oracle Identity and Access Management Deployment Response File`. You can change this.
   - **Response File Version**: The Oracle Identity and Access Management Deployment Wizard provides a default value, which you can change. You can use this to keep track of different file versions.

- **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.

Click **Next**. The Select IAM Products screen appears.

6. On the Select IAM Products screen, select the type of deployment that you would like to perform. The following options are available:
   - **Oracle Identity Manager (OIM) Only**: Select this option to install and configure Oracle Identity Manager and SOA with Oracle HTTP Server.
   - **Oracle Access Manager (OAM) Suite Only**: Select this option to install and configure Oracle Access Management suite with Webgate and Oracle HTTP Server.
   - **OIM-OAM Integrated and Oracle Unified Directory (OUD)**: Select this option to install and configure the following products:
     - Oracle Identity Manager
     - Oracle SOA
     - Oracle Access Management
     - Oracle Unified Directory
     - Oracle HTTP Server
     - Webgate

   Note: After you select IAM components that 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, you must cancel this wizard, and restart the Oracle Identity and Access Management Deployment Wizard.

   Click **Next**. The Select Topology screen appears.

7. On the Select Topology screen, select the **Single Node** option. In the Host Name field, specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.

   Click **Next**. The Select Installation and Configuration Locations screen appears.

8. Use the Select Installation and Configuration Locations screen to supply the location of the various directories required for installation and configuration actions.
   - **Lifecycle Management Store Location**: This is a location for storing data to support lifecycle management, for example: `/u01/lcm` (*`LCM_HOME`*)

     Log files are present under the logs directory in *`LCM_HOME`*. On Linux, this is located at *`LCM_HOME`*`/provisioning/logs`.

- **Software Repository Location**: This is the location of the Deployment repository, for example: `/u01/lcm/Repository`
- **Software Installation Location**: Specify the location where you want the Middleware Homes to be placed.

  Ensure that this directory path is 45 characters or fewer in length. A longer pathname can cause errors during Oracle Identity and Access Management deployment. See Section 8.2.1, "Null Error Occurs When WebLogic Patches Are Applied."
- **Shared Configuration Location**: Specify the location of shared configuration, for example: `/u01/oracle/config` (*`SHARED_CONFIG_DIR`*). (In a single host environment, the shared configuration location is not actually shared.)

Click **Next**. The Set User Names and Passwords screen appears.

9. The Set User Names and Passwords screen shows the users that will be created during the deployment process. You can either set a common password for all of the user accounts listed, or set individual passwords as required for each of the accounts. It is also possible to change some of the default usernames that are created, if desired.
   - **Enter Common IAM Password**: Enter a common IAM password. This is the default password that will be used by all accounts unless overriden on an account by account basis.
   - **Confirm Common IAM Password**: Confirm the password.
   - If you want to override the default usernames and common password, then select the **Modify the Username and Password for the user accounts** option. Select **Edit** next to the account you wish to modify, and override the Username and Password as desired.

   Click **Next**.
10. The Configure Oracle Unified Directory screen appears.

    Note: This screen will appear only if you selected the OIM-OAM Integrated and Oracle Unified Directory (OUD) option on the Select IAM Products screen.

    Use the Configure Oracle Unified Directory screen to select configuration options for Oracle Unified Directory.

    Oracle Unified Directory Configuration Parameters

    - **First OUD Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
    - **Port of First OUD Instance**: Specify the non-SSL port number to be used by Oracle Unified Directory.
    - **SSL Port of First OUD Instance**: Specify the SSL port to be used for the first instance of Oracle Unified Directory.
    - **Identity Store Realm DN**: Specify the Distinguished Name of the Oracle Unified Directory realm, for example: `dc=mycompany,dc=com`

    Click **Next**. The Configure Oracle HTTP Server screen appears.

11. Use the Configure Oracle HTTP Server screen to change the installation ports used for Oracle HTTP Server (OHS).

    Oracle HTTP Server Configuration Parameters

    - **Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
    - **HTTP Port**: Specify the non-SSL port number to be used for the Oracle HTTP Server.
    - **SSL Port**: Specify the SSL port number to be used for the Oracle HTTP Server.
    - **OAM Admin Front End Port**: This field is purely informational. This value points to the HTTP port value.
    - **OIM Admin Front End Port**: Specify the port to be used by the Oracle Identity Manager Administration Server.
    - **Instance Name**: This field is purely informational. It displays the instance name of the Oracle HTTP Server.

    Click **Next**.

12. The Configure Oracle Identity Manager screen appears.

    Note: This screen will appear only if you selected one of the following options on the Select IAM Products screen:

    - **Oracle Identity Manager (OIM) Only**
    - **OIM-OAM Integrated and Oracle Unified Directory (OUD)**

    Use the Configure Oracle Identity Manager screen to modify the ports used by Oracle Identity Manager and, optionally, to configure an email server.

    Oracle Identity Manager Configuration Parameters

    - **OIM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology.
    - **Admin Server Port**: The port number that the IAMGovernanceDomain Admin Server will use, for example: `7101`
    - **Port**: Specify the port to be used by the Oracle Identity Manager managed server, for example: `14000`
    - **Configure Email Server**: Select this if you want to configure OIM to send Email Notifications. If you select **Configure Email Server**, you must provide the following details:
      - **Outgoing Server Name**: Specify the name of your outgoing email server, for example: `email.mycompany.com`
      - **Outgoing Server Port**: Specify the port that your outgoing email server uses, for example: `465`
      - **Outgoing Email Security**: The security used by SMTP server. Select an option from the drop-down list. Possible values are `None`, `TLS` and `SSL`.
      - **Username**: If you require a username to authenticate with the email server, enter that username.
      - **Password**: Enter the password for the username.

Click **Next**.

13. The Configure Oracle Identity Manager Database screen appears.

> **Note:** This screen is displayed only if you selected one of the following options on the Select IAM Products screen:
>
> - **Oracle Identity Manager (OIM) Only**
> - **OIM-OAM Integrated and Oracle Unified Directory (OUD)**

Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains the schemas for Oracle Identity Manager, SOA, and Oracle Platform Security Services.

Oracle Identity Manager (OIM) Database Configuration

- **Schema Prefix**: Specify the prefix that you want to use for the OIM schema. The schema prefix should be the same as the one that you provided when running the RCU.

  The default value of this field is `DEV`. This value can be edited.

- **Schema User Name**: This field specifies the name of the schema user.

  The value of this field depends on the **Schema Prefix** value. This field takes the value of **Schema Prefix** and adds an OIM suffix to it. For example, `DEV_OIM`.

- **Service Name**: Specify the service name of the database service, for example: `oimdb.mycompany.com`

- **Schema Password**: Specify the password you used when creating the Oracle Identity Manager and SOA schemas using the Oracle Identity and Access Management RCU.

- **Single Instance Database**: Select if you are using a single Oracle Database.
  - **Host Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.

- **RAC Database**: Select if you are using an Oracle RAC Database.
  - **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com`.
  - **Scan Port**: Enter the port used by the Grid Infrastructure Listener, for example: `1521`.
  - **ONS Scan Address**: Defaults to the scan address.
  - **ONS Port**: Determine the ONS port by using the RAC `srvctl` command on the Oracle Database server, as shown in the following example:

    ```
    srvctl config nodeapps -s
    ONS exists: Local port 6100, remote port 6200, EM port 2016
    ```

Click **Next**.

14. The Configure SOA screen appears.

Note: This screen is displayed only if you selected one of the following options on the Select IAM Products screen:

- **Oracle Identity Manager (OIM) Only**
- **OIM-OAM Integrated and Oracle Unified Directory (OUD)**

Use the Configure SOA screen to enter the ports to be used by the SOA Managed server.

SOA Configuration Parameters

- **SOA Host**: This field is purely informational
- **Port**: Specify the port number to be used by the SOA Server.

Click **Next**.

15. The Configure Oracle Access Manager screen appears.

Note: This screen is displayed only if you selected one of the following options on the Select IAM Products screen:

- **Oracle Access Manager (OAM) Suite Only**
- **OIM-OAM Integrated and Oracle Unified Directory (OUD)**

On the Configure Oracle Access Manager screen, enter the following information:

Oracle Access Management Suite Configuration Parameters

- **OAM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
- **Admin Server Port**: The Port that the IAMAccessDomain Admin Server will use, for example: `7001`
- **OAM Port**: Specify the port number to be used by OAM Managed Server.
- **OAM Transfer Mode**: This field is purely informational.
- **Cookie Domain**: Specify the cookie domain. For example: `.mycompany.com`

Click **Next**.

16. The Configure Oracle Access Manager Database screen appears.

Use the Configure Oracle Access Manager Database screen to enter information about the Database that contains the schemas for Oracle Access Manager.

Note: This screen is displayed only if you selected one of the following options on the Select IAM Products screen:

- **Oracle Access Manager (OAM) Suite Only**
- **OIM-OAM Integrated and Oracle Unified Directory (OUD)**

- **Schema Prefix**: Specify the prefix that you want to use for the OAM schema. The schema prefix should be the same as the one that you provided when running the RCU.

  The default value of this field is `DEV`. This value can be edited.

- **Schema User Name**: This field specifies the name of the schema user.

  The value of this field depends on the **Schema Prefix** value. This field takes the value of **Schema Prefix** and adds an OAM suffix to it. For example, `DEV_OAM`.

- **Service Name**: Specify the service name of the database service, for example: `oamdb.mycompany.com`
- **Schema Password**: Specify the password you used when creating the Oracle Access Manager schema using the Oracle Identity and Access Management RCU.
- **Single Instance Database**: Select if you are using a single Oracle Database.
  - **Host Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC Database**: Select if you are using an Oracle RAC Database.
  - **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com`.
  - **Scan Port**: Enter the port used by the Grid Infrastructure Listener, for example: `1521`.
  - **ONS Port**: Determine the ONS port by using the RAC `srvctl` command on the Oracle Database server, as shown in the following example:

    ```
    srvctl config nodeapps -s
    ONS exists: Local port 6100, remote port 6200, EM port 2016
    ```

Click **Next**.

17. 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.

    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 a Multi-Host Topology

Complete the steps described in this section to create a new Deployment Response File for a multi-host topology. This section includes the following topics:

4.4.1 Creating a Deployment Response File for Only Oracle Identity Manager with HA

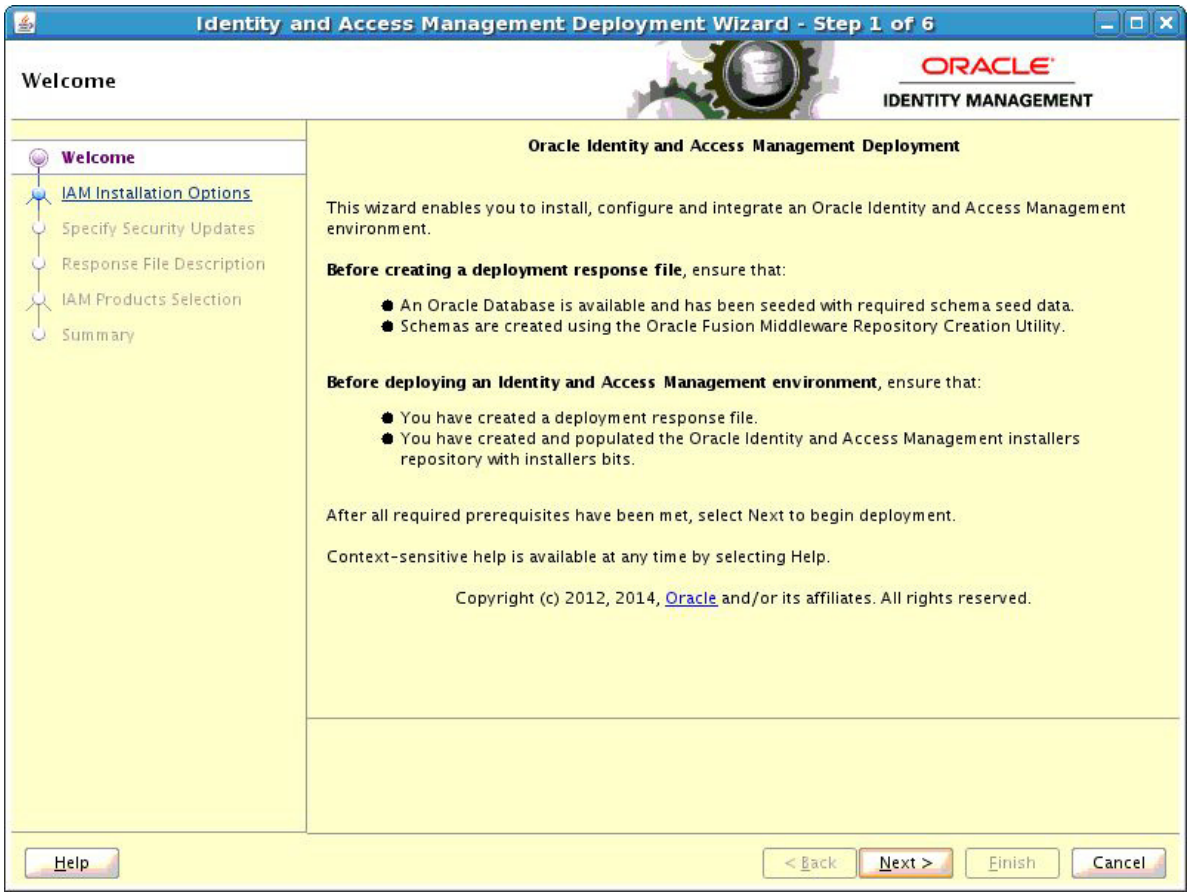
This section outlines the tasks you must perform to set up only Oracle Identity Manager with High Availability (HA). It includes the following topics:

4.4.1.1 Welcome

Start the Deployment Wizard by performing the steps in Section 4.2, "Starting the Identity and Access Management Deployment Wizard". After you complete those steps, the Welcome screen appears

Use the Welcome screen to learn more about the wizard, including some prerequisites for using it.

The Welcome screen provides a brief overview of the wizard and lists some requirements that must be met.



Click **Next**.

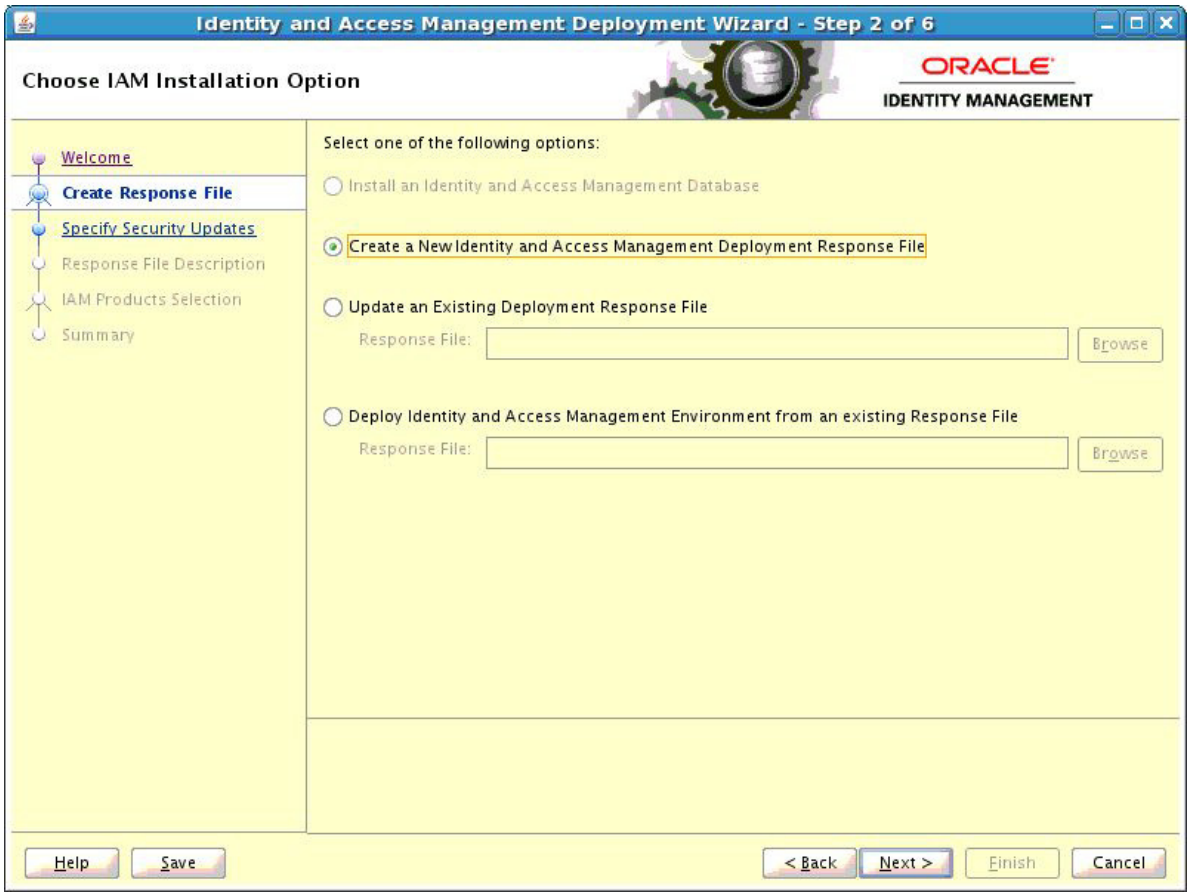
4.4.1.2 Specify Inventory Directory

If you are presented with the Specify Inventory Directory screen, proceed as described in Step 2 in Section 2.8, "Installing the Oracle Identity and Access Management Lifecycle Tools."

Click **OK**.

4.4.1.3 Choose IAM Installation Options

Select **Create a New Identity and Access Management Environment Deployment Response File** if you are creating a response file for the first time.

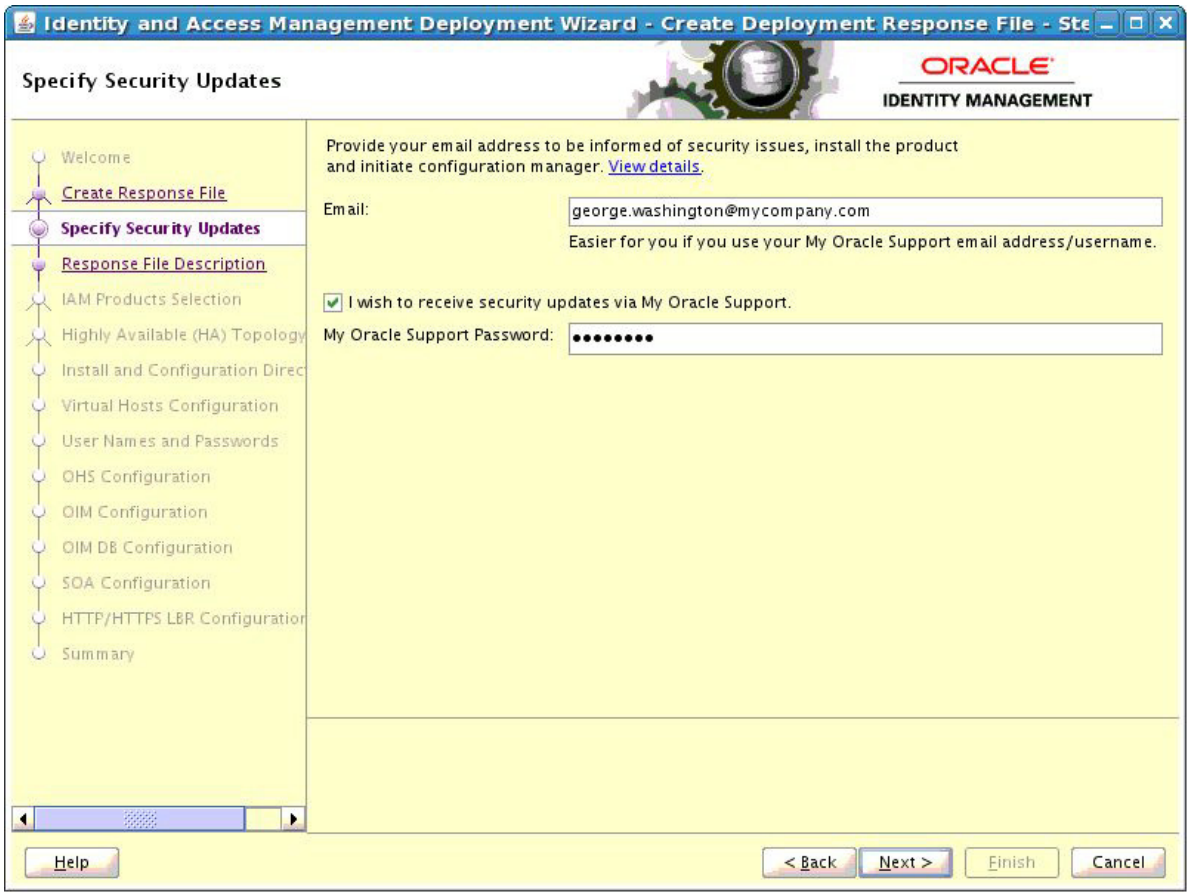


Click **Next**.

4.4.1.4 Specify Security Updates

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 email 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.

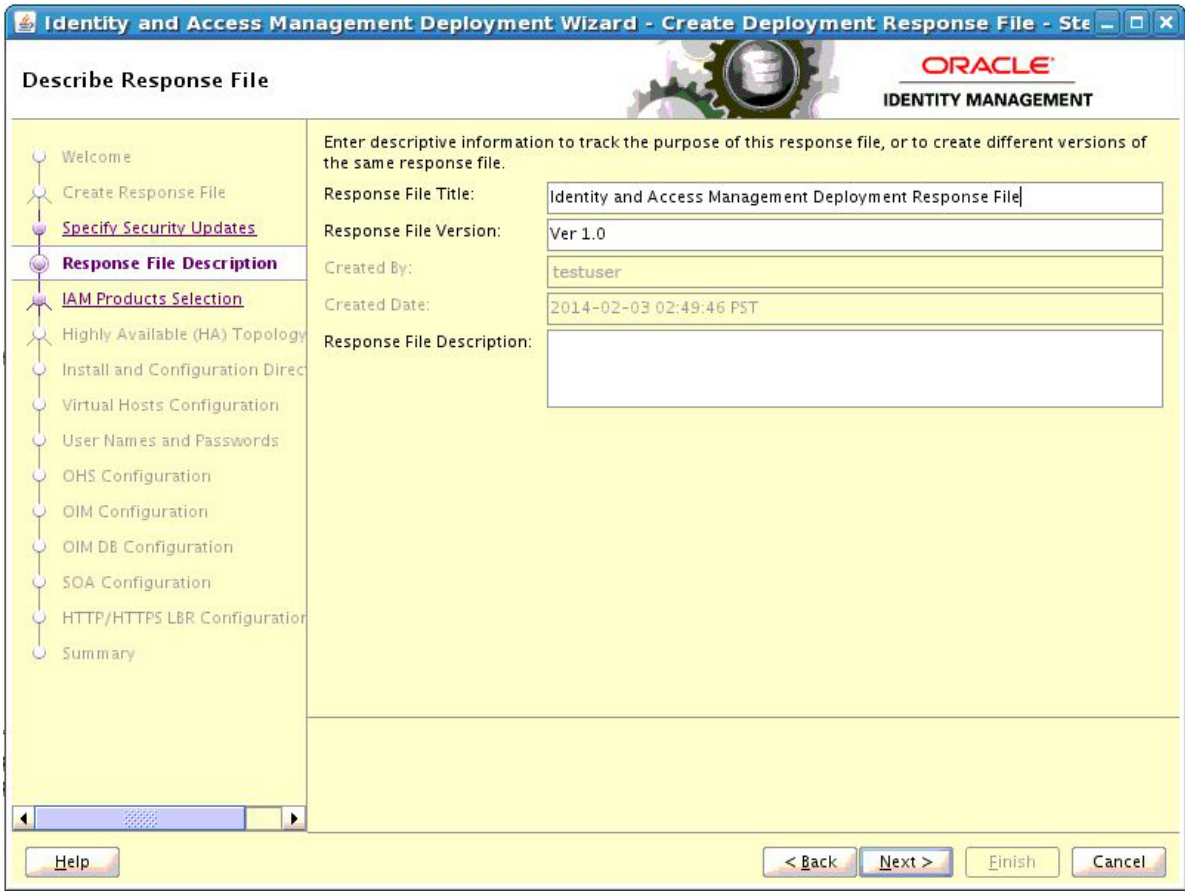


Click **Next**.

4.4.1.5 Describe Response File

Specify descriptive information to identify the response file. The information entered on this screen is metadata information. This information can be used to uniquely identify a response file if multiple response files are created.

- **Response File Title**: The Oracle Identity and Access Management Deployment Wizard provides the default title `Oracle Identity and Access Management Deployment Response File`. You can change this.
- **Response File Version**: The Oracle Identity and Access Management Deployment Wizard provides a default value, which you can change. You can use this to keep track of different file versions.
- **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.



Click **Next**.

4.4.1.6 Select IAM Products

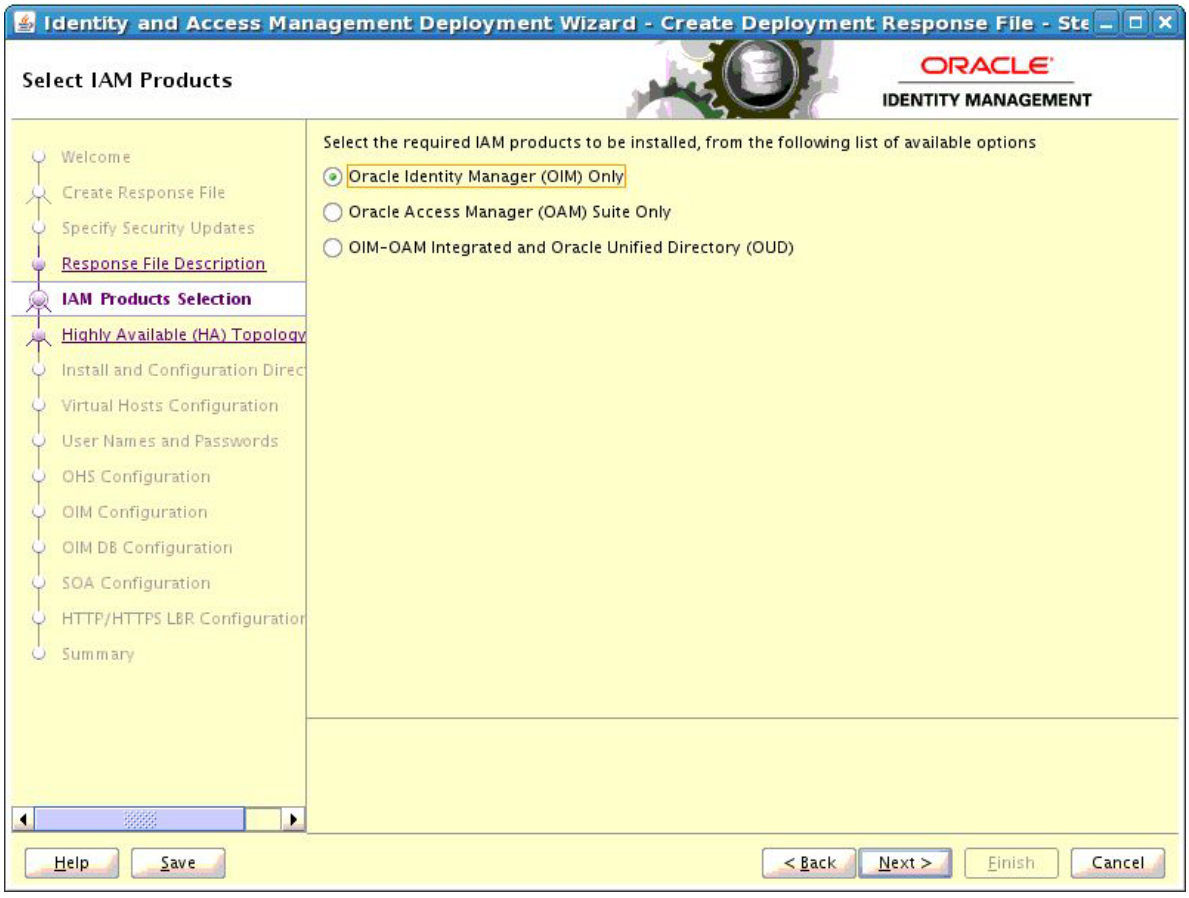
On the Select IAM Products screen, select the type of deployment that you would like to perform. The following options are available:

- **Oracle Identity Manager (OIM) Only**: Select this option to install and configure Oracle Identity Manager and SOA with Oracle HTTP Server.
- **Oracle Access Manager (OAM) Suite Only**: Select this option to install and configure Oracle Access Management suite with Webgate and Oracle HTTP Server.
- **OIM-OAM Integrated and Oracle Unified Directory (OUD)**: Select this option to install and configure the following products:
  - Oracle Identity Manager
  - Oracle SOA
  - Oracle Access Management
  - Oracle Unified Directory
  - Oracle HTTP Server
  - Webgate

Note: If you want to deploy a multiple host topology using the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option, then do not use this guide. This guide covers only the following HA deployments:

- **Oracle Identity Manager (OIM) Only**
- **Oracle Access Manager (OAM) Suite Only**

For performing an HA deployment using you using the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option, you must refer to *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.



Note: After you select IAM components that 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, you must cancel this wizard, and restart the Oracle Identity and Access Management Deployment Wizard.

Click **Next**.

4.4.1.7 Select Topology

Use the Select Topology screen to select configuration options and provide information about hosts and products.

- **Single Node**: Select this option to deploy a simple, single host topology.
  - **Host Name**: Specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.
- **Highly Available (HA)**: This option enables you to deploy a multiple host topology. Select this option to perform an HA deployment.

  You must provide the following information:

  Note: All host names must be fully qualified.

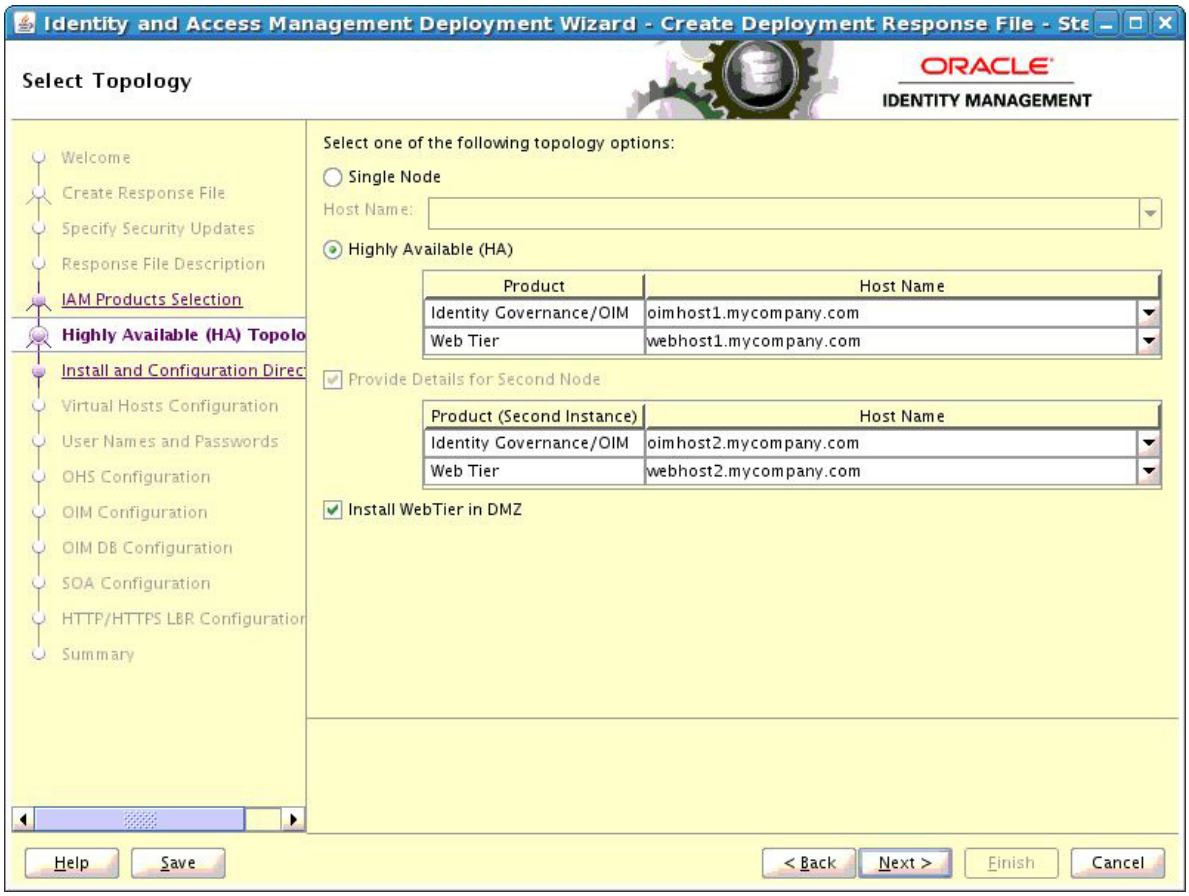
  The products that are listed under the Product column depends on the option that you selected on the "Select IAM Products" screen.

  - **Identity Governance /OIM**: Specify the fully qualified host name which will be running Oracle Identity Manager. For example, `OIMHOST1.mycompany.com`
  - **Web Tier**: Specify the fully qualified host name which will be running the Oracle HTTP server and WebGate. For example, `WEBHOST1.mycompany.com`

  Ensure **Provide Details for Second Node** is selected, then enter the following information:

  - **Identity Governance (OIM)**: Specify the fully qualified host name which will be running the second instance of Oracle Identity Manager. For example, `OIMHOST2.mycompany.com`
  - **Web Tier**: Specify the fully qualified host name which will be running the second instance of Oracle HTTP server and WebGate. For example, `WEBHOST2.mycompany.com`

  Note: After you select the topology option, do not click the **Back** button in the subsequent screens to modify your topology options. If you need to make any modification in the previous screens, you must cancel this wizard, and restart the Oracle Identity and Access Management Deployment Wizard.



Click **Next**.

4.4.1.8 Select Installation and Configuration Locations

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

- **Lifecycle Management Store Location**: This is a location for storing data to support lifecycle management, for example: `/u01/lcm` (*LCM_HOME*)

  Log files are present under the logs directory in *LCM_HOME*. On Linux, this is located at *LCM_HOME*`/provisioning/logs`.

  > **Note:** You should mount the *LCM_HOME* directory on every host for the duration of Identity and Access Management Deployment. If you have done this, select the **Mounted on Web hosts** option.
  >
  > If, however, you cannot mount the directory for the duration of provisioning, you can still perform deployment, but you must also perform some manual steps. See Section 5.3, "Deploying Identity and Access Management Without a Common LCM_HOME" for details.

- **Mounted on Web hosts**: If you have mounted your *LCM_HOME* directory on your web hosts then, select Mounted on Web hosts.
- **Software Repository Location**: This is the location of the Deployment repository, for example: `/u01/lcm/Repository`

- **Software Installation Location**: This is the location on shared storage under where you want the Middleware Home to be placed, for example: `/u01/oracle`

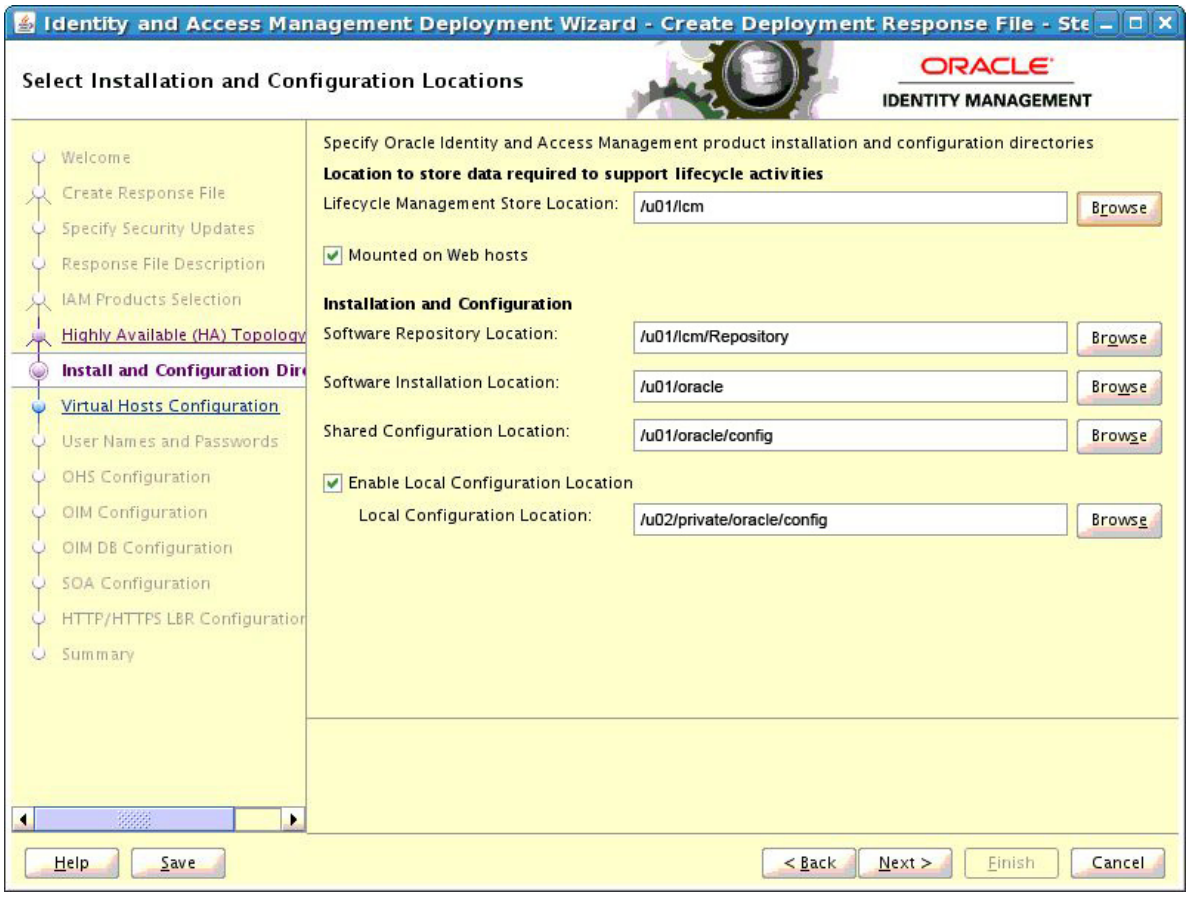
  Ensure that this directory path is 45 characters or fewer in length. A longer pathname can cause errors during Oracle Identity and Access Management deployment. See Section 8.2.1, "Null Error Occurs When WebLogic Patches Are Applied."

- **Shared Configuration Location**: Specify the location of shared configuration, for example: `/u01/oracle/config` (*`SHARED_CONFIG_DIR`*).

- **Enable Local Configuration Location**: Select this option to enable local configuration.

- **Local Configuration Location**: This is the location on local storage where the OIM managed servers, SOA managed servers, and the OHS instances are stored, for example: `/u02/private/oracle/config`.

> **Note:** The Identity and Access Management process requires that you use the same Deployment profile on all hosts in the deployment. Therefore, the locations you enter on this screen must be consistent across all hosts.



Click **Next**.

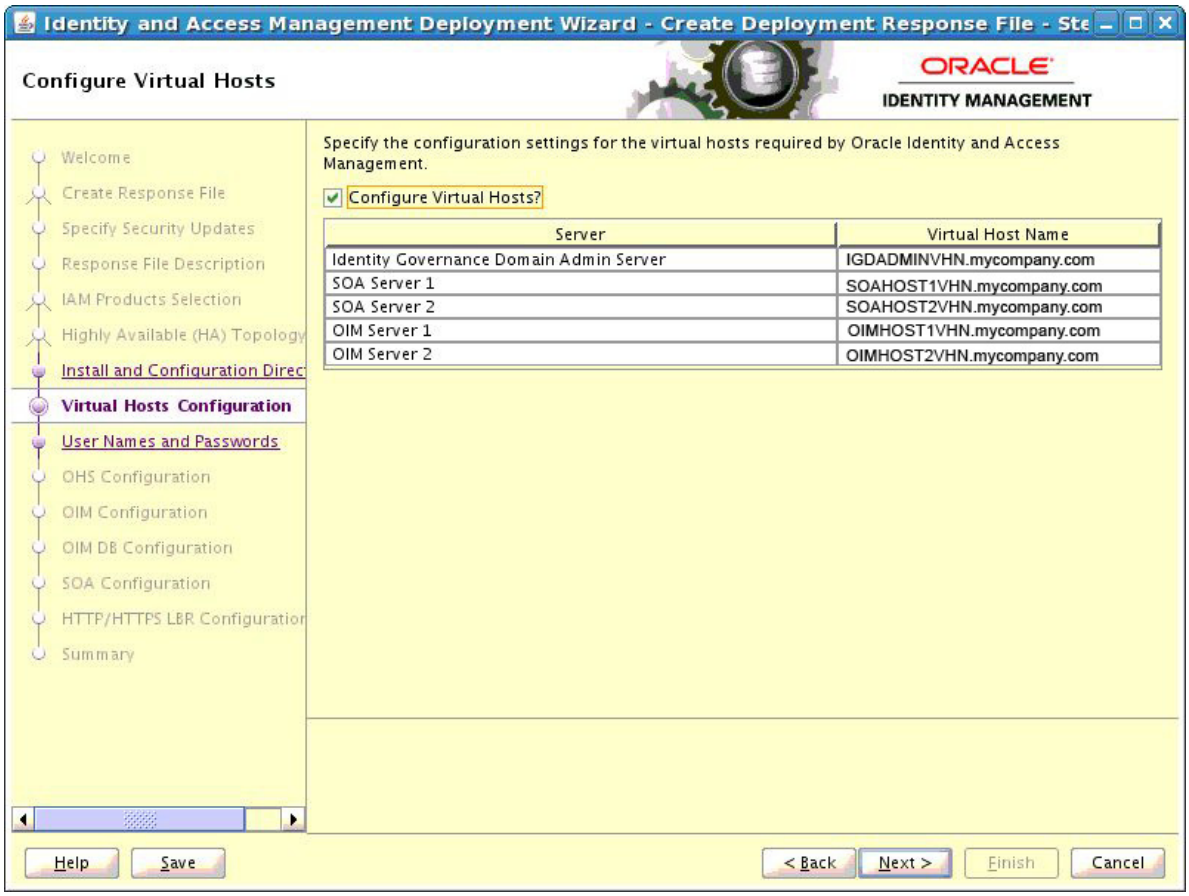
4.4.1.9 Configure Virtual Hosts (Optional)

If you want to configure virtual hosts, then on the Configure Virtual Hosts screen, select the **Configure Virtual Hosts** check box, and provide the virtual host names for the servers listed on the screen.

You can provide a virtual host for the Administration Server, SOA server and OIM server. These virtual servers should be resolved either through DNS or through the `/etc/hosts` file.

Enter the **Virtual Host Name** for each **Server** in the topology, for example:

- **Governance Domain Admin Server**: `IGDADMINVHN.mycompany.com`
- **SOA Server**: `SOAHOST1VHN.mycompany.com`
- **SOA Server 2**: `SOAHOST2VHN.mycompany.com`
- **OIM Server**: `OIMHOST1VHN.mycompany.com`
- **OIM Server 2**: `OIMHOST2VHN.mycompany.com`

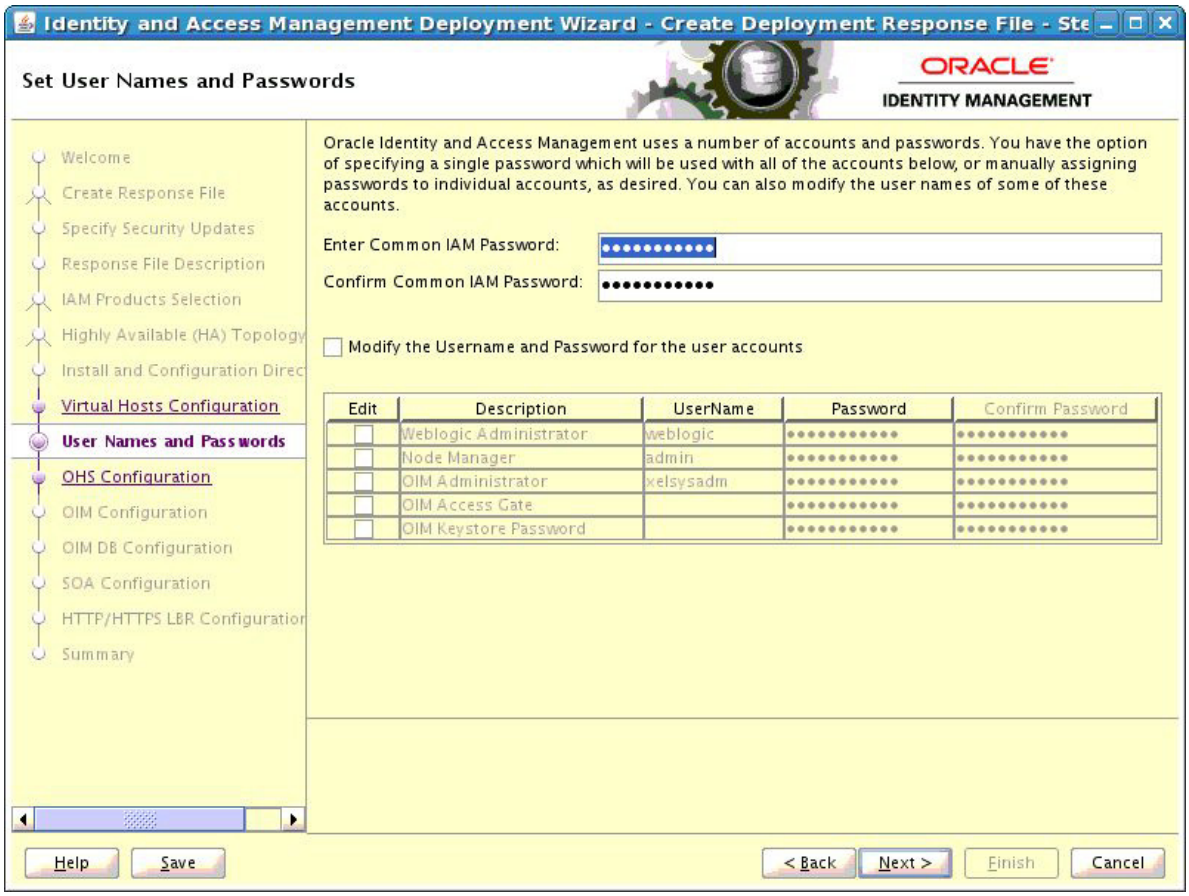


Click **Next**.

4.4.1.10 Set User Names and Passwords

The Set User Names and Passwords screen shows the users that will be created during the deployment process. You can either set a common password for all of the user accounts listed, or set individual passwords as required for each of the accounts. It is also possible to change some of the default usernames that are created, if desired.

- **Enter Common IAM Password**: Enter a common IAM password. This is the default password that will be used by all accounts unless overriden on an account by account basis.
- **Confirm Common IAM Password**: Re-enter the password.
- If you want to override the default usernames and common password, then select the **Modify the Username and Password for the user accounts** option. Select **Edit** next to the account you wish to modify, and override the Username and Password as desired.



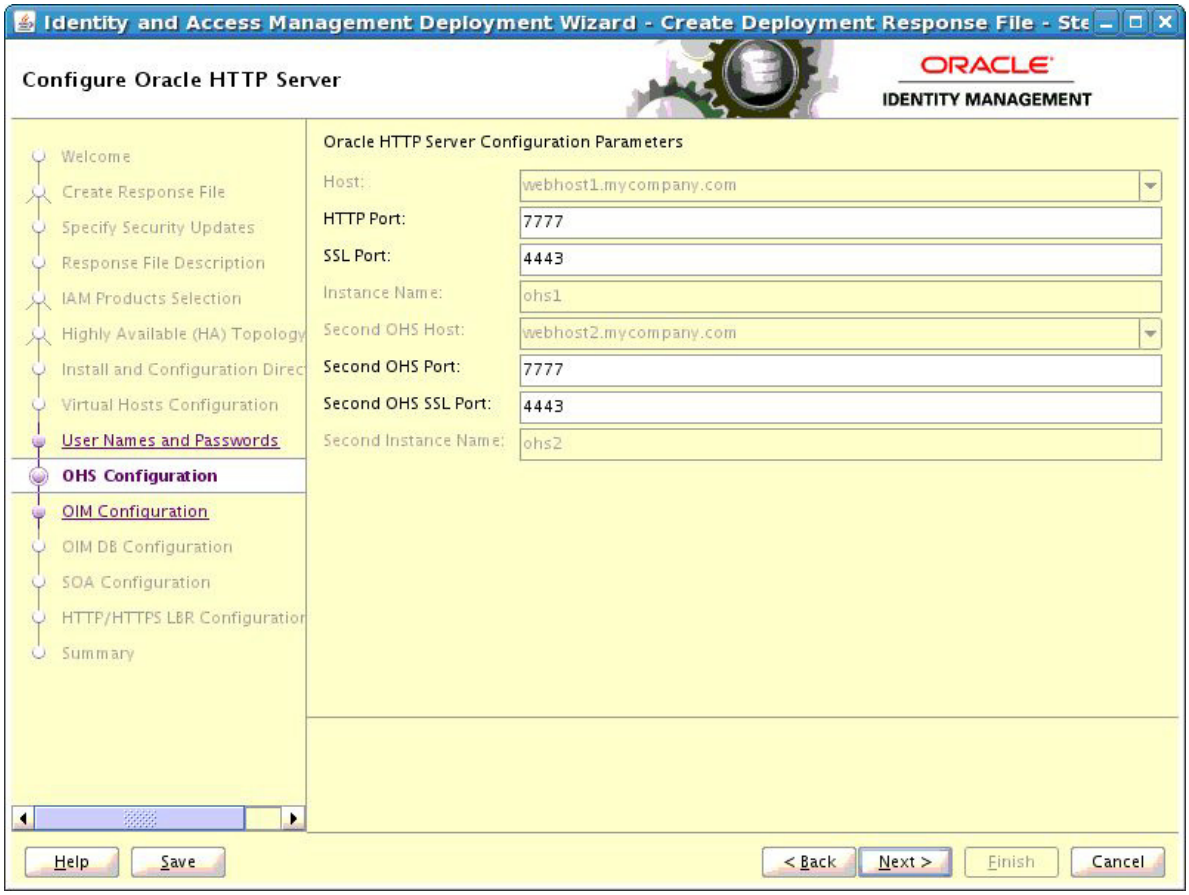
Click **Next**.

4.4.1.11 Configure Oracle HTTP Server

Use the Configure Oracle HTTP Server screen to change the installation ports used for Oracle HTTP Server (OHS).

- **Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
- **HTTP Port**: Specify the non-SSL port number to be used for the Oracle HTTP Server.
- **SSL Port**: Specify the SSL port number to be used for the Oracle HTTP Server.
- **Instance Name**: This field is purely informational. It displays the instance name of the Oracle HTTP Server.

- **Second OHS Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
- **Second OHS Port**: Specify the non-SSL port number to be used for the second instance of Oracle HTTP Server.
- **Second OHS SSL Port**: Specify the SSL port number to be used for the second instance of Oracle HTTP Server.
- **Second Instance Name**: This field is purely informational. It displays the second instance name of the Oracle HTTP Server.

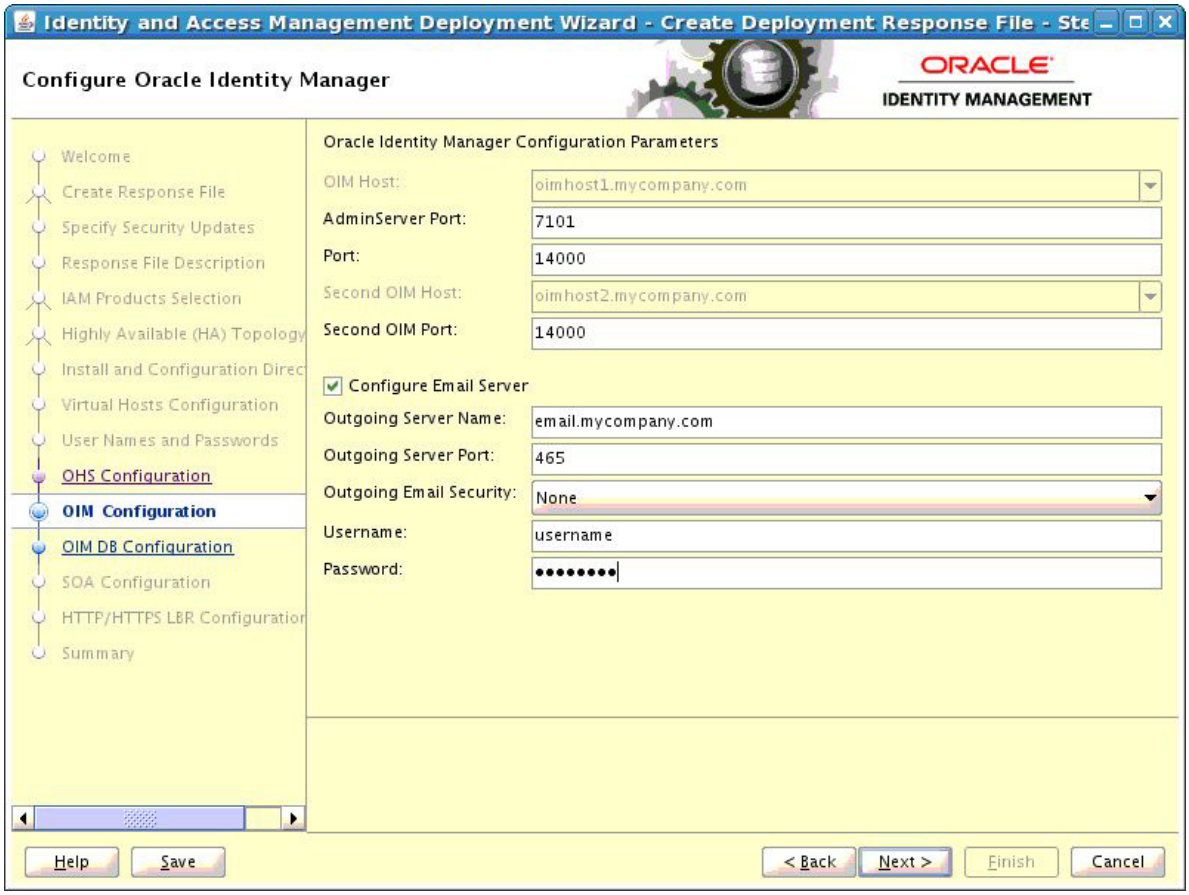


4.4.1.12 Configure Oracle Identity Manager

Use the Configure Oracle Identity Manager screen to modify the ports used by Oracle Identity Manager and, optionally, to configure an email server.

- **OIM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology.
- **Admin Server Port**: The port number that the IAMGovernanceDomain Admin Server will use, for example: `7101`
- **Port**: Specify the port to be used by the first instance of Oracle Identity Manager managed server, for example: `14000`
- **Second OIM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology.
- **Second OIM Port**: Specify the port number to be used by the second instance of OIM Managed Server, for example: `14000`

- **Configure Email Server**: Select this if you want to configure OIM to send Email Notifications. If you select **Configure Email Server**, you must also select **Configure Email Server** and provide the following details:
  - **Outgoing Server Name**: Specify the name of your outgoing email server, for example: `email.mycompany.com`
  - **Outgoing Server Port**: Specify the port that your outgoing email server uses, for example: `465`
  - **Outgoing Email Security**: The security used by SMTP server. Select an option from the drop-down list. Possible values are `None`, `TLS` and `SSL`.
  - **Username**: If you require a username to authenticate with the email server, enter that username.
  - **Password**: Enter the password for the username.



Click **Next**.

4.4.1.13 Configure Oracle Identity Manager Database

Use the Configure Oracle Identity Manager Database screen to enter information about the Database that contains the schemas for Oracle Identity Manager, SOA, and Oracle Platform Security Services.

- **Schema Prefix**: Specify the prefix that you want to use for the OIM schema. The schema prefix should be the same as the one that you provided when running the RCU.

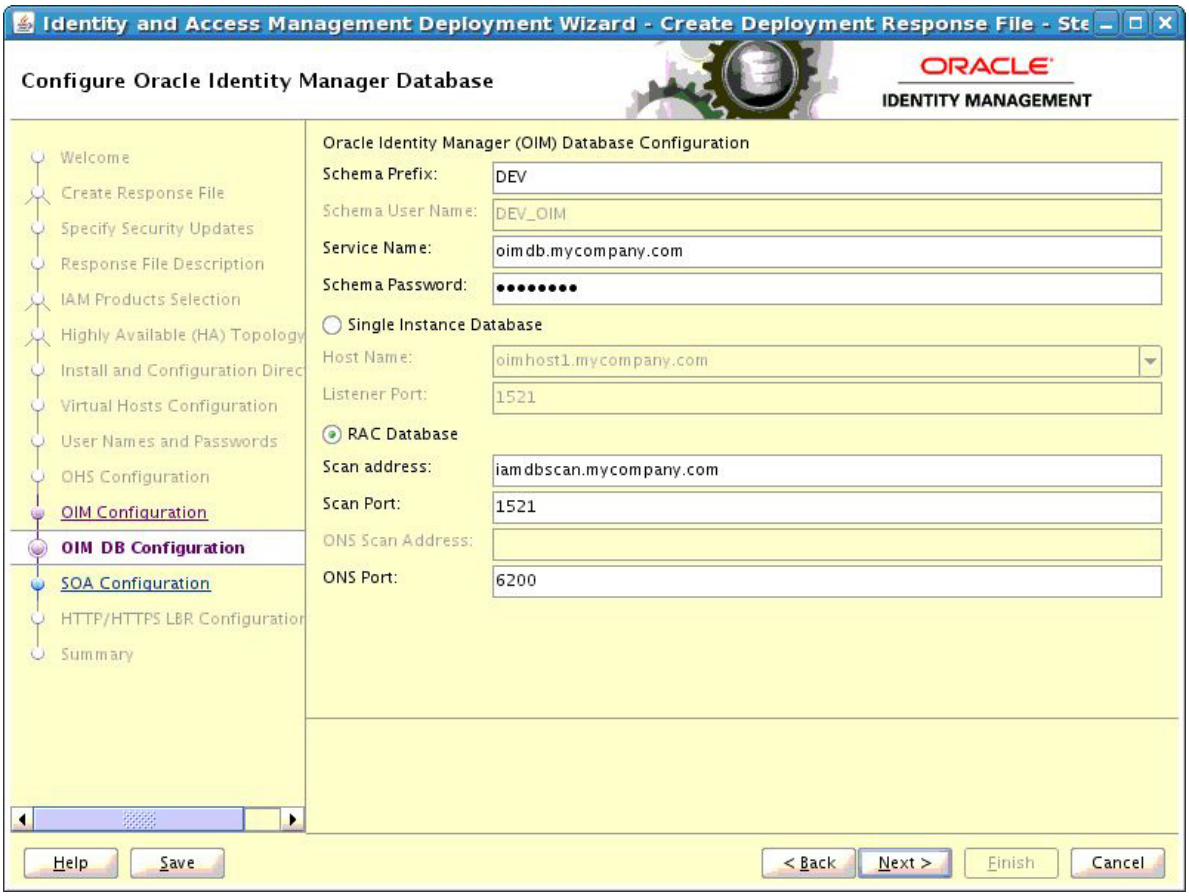
The default value of this field is `DEV`. This value can be edited.

- **Schema User Name**: This field specifies the name of the schema user.

  The value of this field depends on the **Schema Prefix** value. This field takes the value of **Schema Prefix** and adds an OIM suffix to it. For example, `DEV_OIM`.

- **Service Name**: Specify the service name of the database service, for example: `oimdb.mycompany.com`
- **Schema Password**: Specify the password you used when creating the Oracle Identity Manager and SOA schemas using the Oracle Identity and Access Management RCU.
- **Single Instance Database**: Select if you are using a single Oracle Database.
  - **Host Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC Database**: Select if you are using an Oracle RAC Database.
  - **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com`.
  - **Scan Port**: Enter the port used by the Grid Infrastructure Listener, for example: `1521`.
  - **ONS Scan Address**: Defaults to the scan address.
  - **ONS Port**: Determine the ONS port by using the RAC `srvctl` command on the Oracle Database server, as shown in the following example:

    ```
    srvctl config nodeapps -s
    ONS exists: Local port 6100, remote port 6200, EM port 2016
    ```

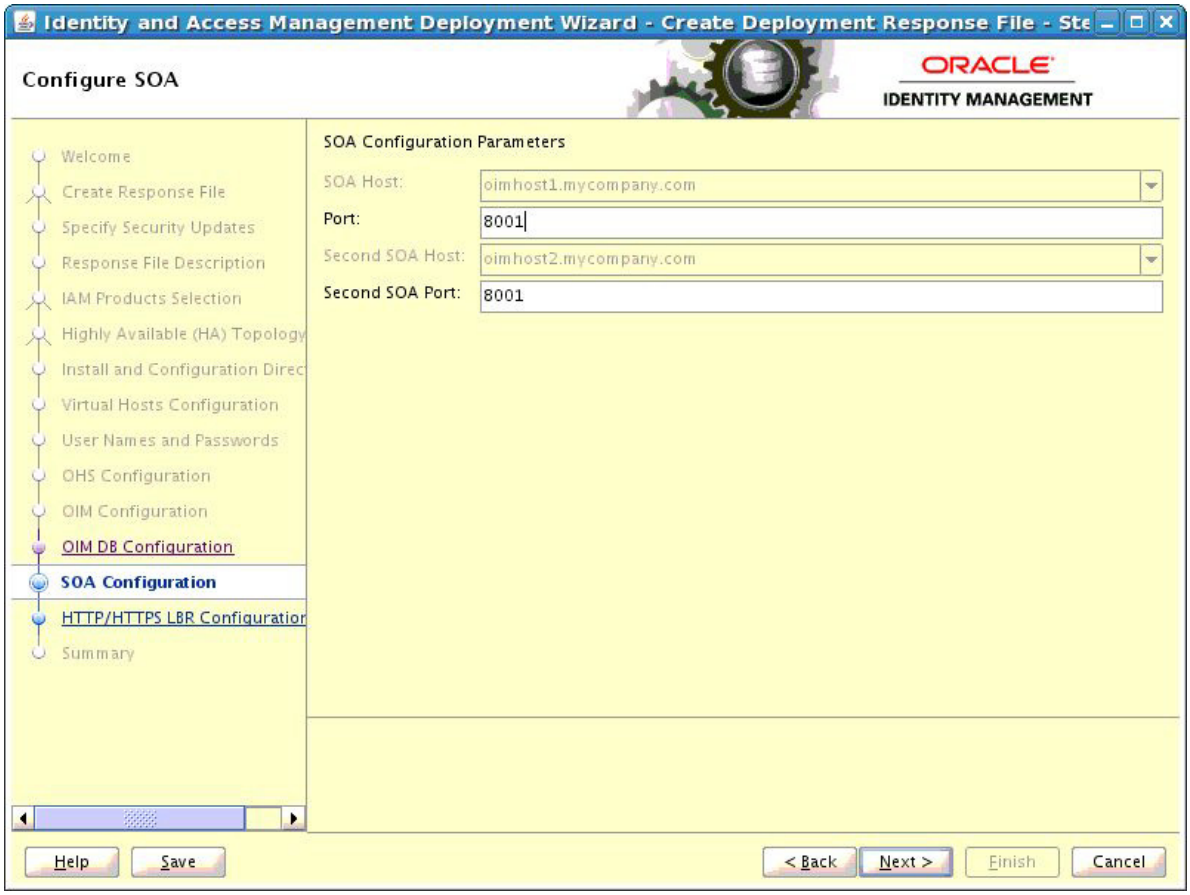


Click **Next**.

4.4.1.14 Configure SOA

Use the Configure SOA screen to enter the ports to be used by the SOA Managed server.

- **SOA Host**: This field is purely informational
- **Port**: Specify the port number to be used by the SOA Managed Server, for example: `8001`.
- **Second SOA Port**: Specify the port number to be used by the second instance of SOA Managed Server, for example: `8001`.



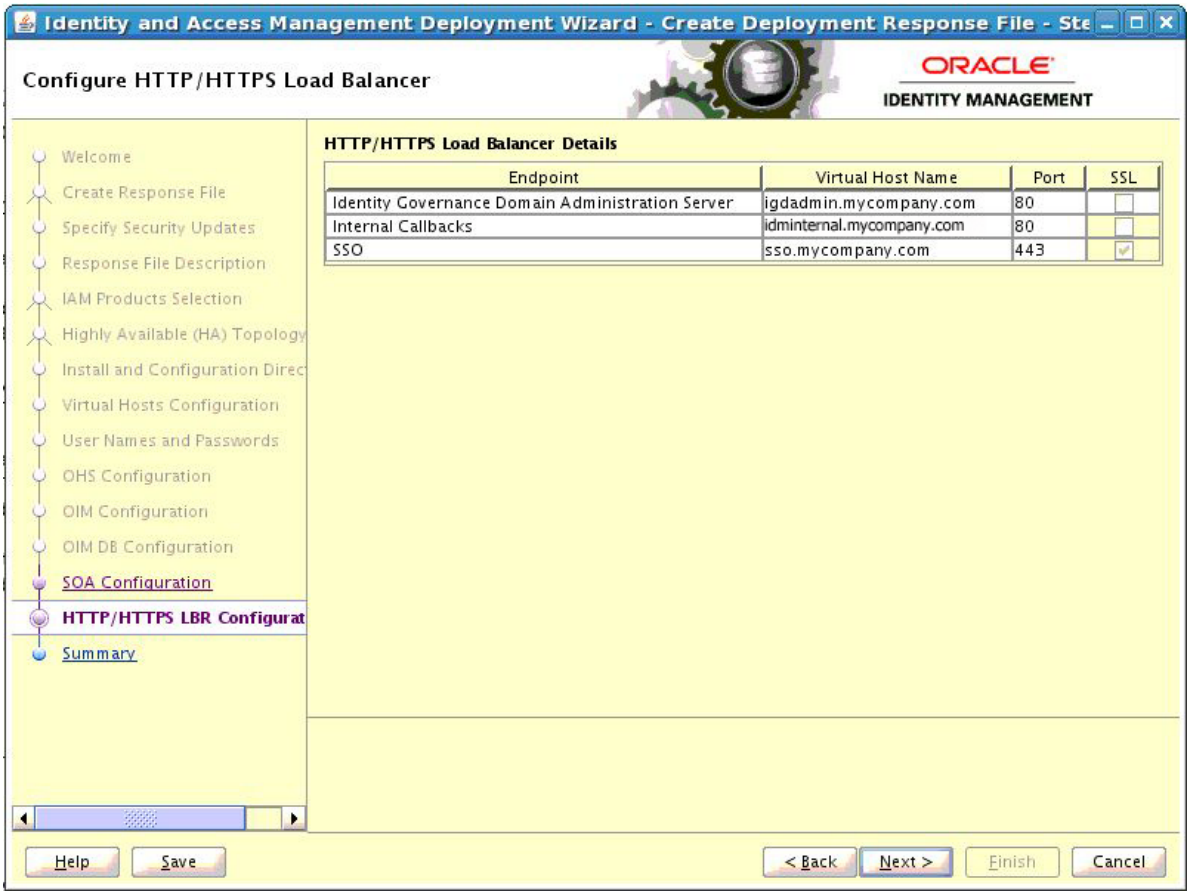
Click **Next**.

4.4.1.15 Configure HTTP/HTTPS Load Balancer

On the HTTP/HTTPS Load Balancer screen, enter details about your load balancer virtual hosts.

Under **HTTP/HTTPS Load Balancer Details**, enter the **Virtual Host Name** and **Port** for each **Endpoint**.

- **IAM Governence Domain Admin**: The Load Balancer end point used to access the IAMGovernanceDomain Administration functions, for example: `igdadmin.mycompany.com`, Port `80`, Not SSL
- **Internal Callbacks**: This is the internal call back virtual host and port, for example: `idminternal.mycompany.com`, Port `80`
- **SSO**: This is the main application entry point, for example: `sso.mycompany.com` Port `443`

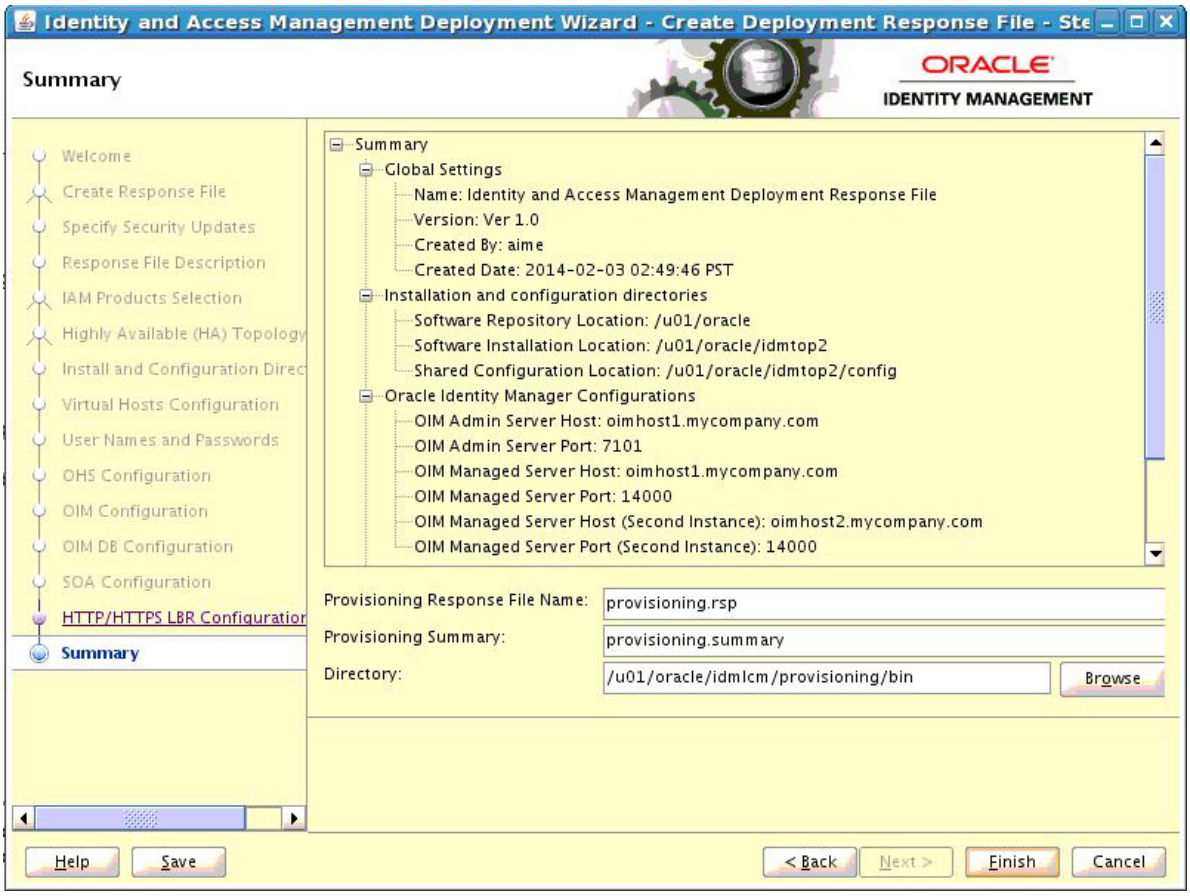


Click **Next**.

4.4.1.16 Summary

Use the Summary screen to view a summary of your selections and enter details about the response file.

- **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.



Click **Finish** to generate the Deployment response file.

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.

4.4.2 Creating a Deployment Response File for Only Access Management with HA

This section outlines the tasks you must perform to set up only Oracle Access Management with High Availability (HA). It includes the following topics:

- Section 4.4.2.1, "Welcome"
- Section 4.4.2.2, "Specify Inventory Directory"
- Section 4.4.2.3, "Choose IAM Installation Options"
- Section 4.4.2.4, "Specify Security Updates"
- Section 4.4.2.5, "Describe Response File"
- Section 4.4.2.6, "Select IAM Products"

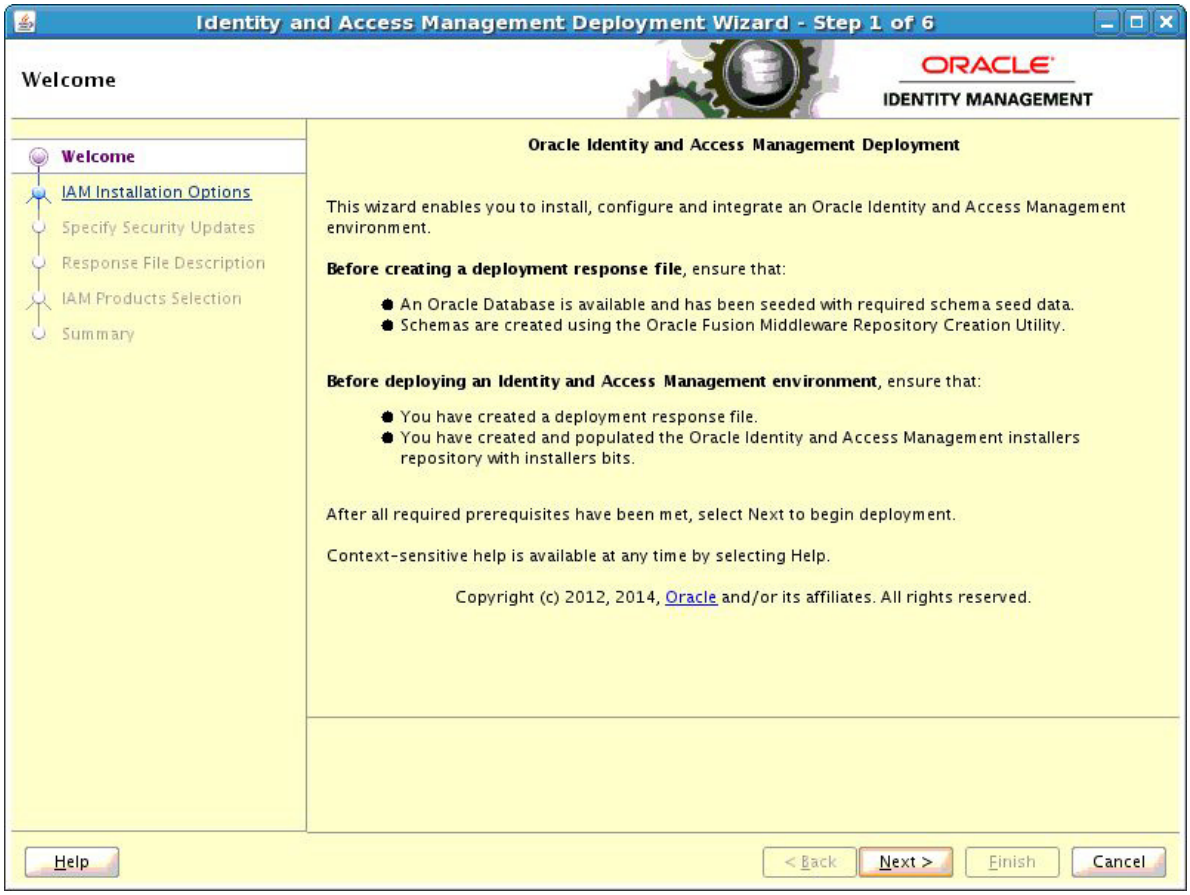
- Section 4.4.2.7, "Select Topology"
- Section 4.4.2.8, "Select Installation and Configuration Locations"
- Section 4.4.2.9, "Configure Virtual Hosts"
- Section 4.4.2.10, "Set User Names and Passwords"
- Section 4.4.2.11, "Configure Oracle HTTP Server"
- Section 4.4.2.12, "Configure Oracle Access Manager"
- Section 4.4.2.13, "Configure Oracle Access Manager Database"
- Section 4.4.2.14, "Configure HTTP/HTTPS Load Balancer"
- Section 4.4.2.15, "Summary"

4.4.2.1 Welcome

Start the Deployment Wizard by performing the steps in Section 4.2, "Starting the Identity and Access Management Deployment Wizard". After you complete those steps, the Welcome screen appears

Use the Welcome screen to learn more about the wizard, including some prerequisites for using it.

The Welcome screen provides a brief overview of the wizard and lists some requirements that must be met.



Click **Next** to continue.

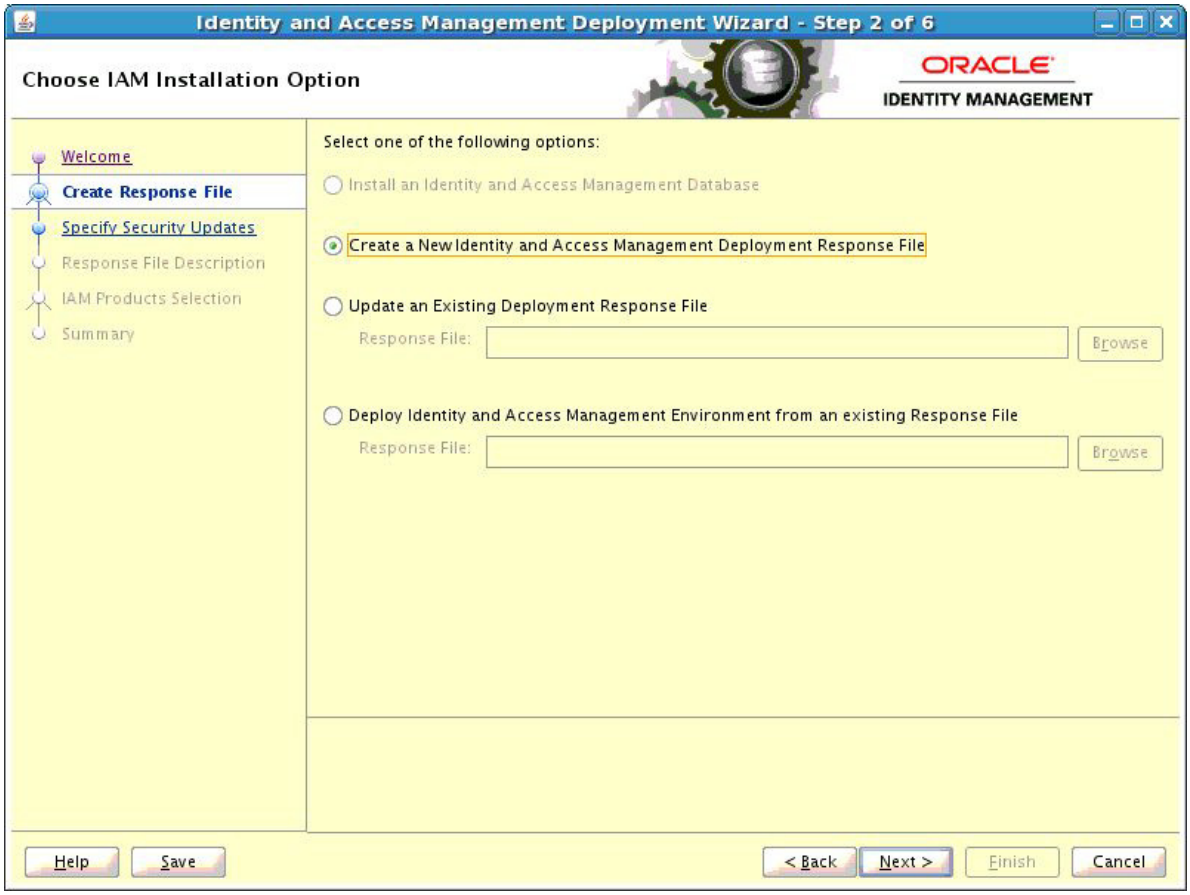
4.4.2.2 Specify Inventory Directory

If you are presented with the Specify Inventory Directory screen, proceed as described in Step 2 in Section 2.8, "Installing the Oracle Identity and Access Management Lifecycle Tools."

Click **OK** to continue.

4.4.2.3 Choose IAM Installation Options

Select **Create a New Identity and Access Management Environment Deployment Response File** if you are creating a response file for the first time.

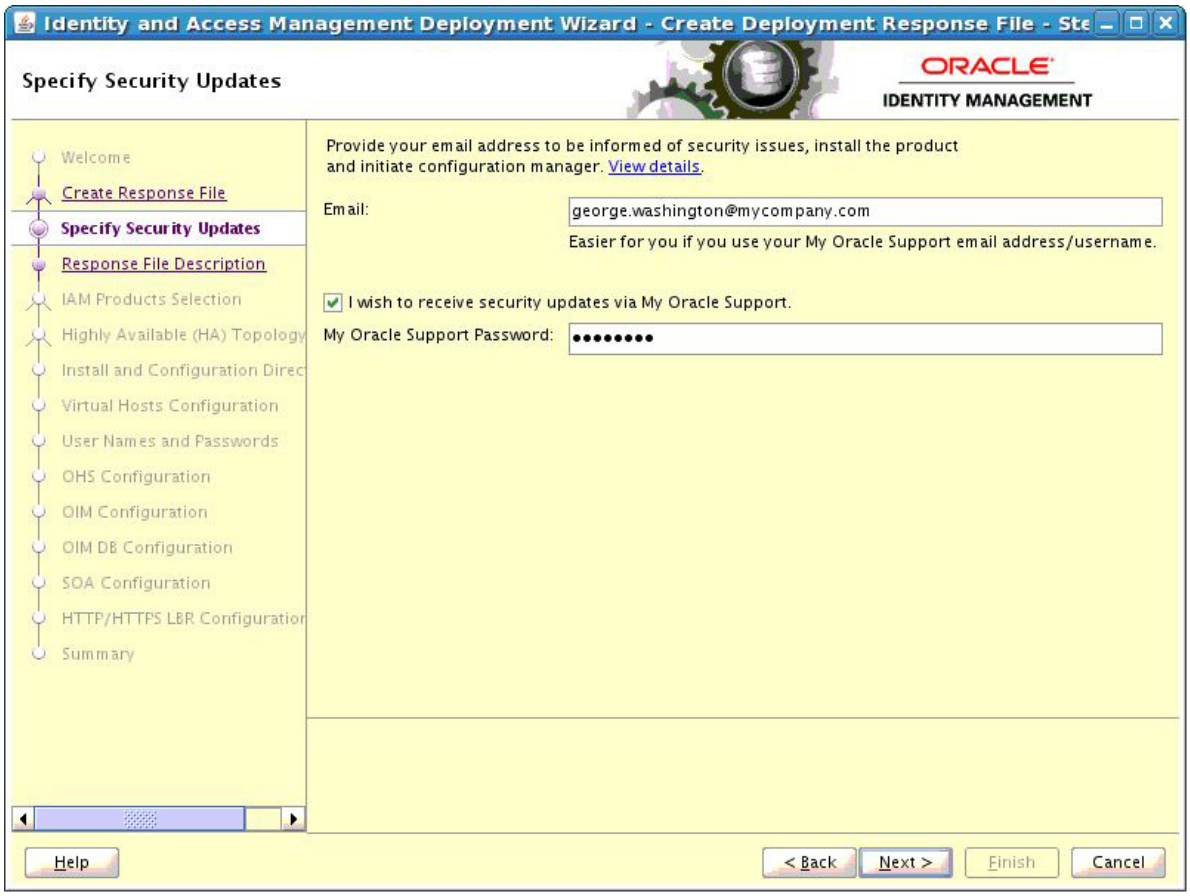


Click **Next** to continue.

4.4.2.4 Specify Security Updates

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 email 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.

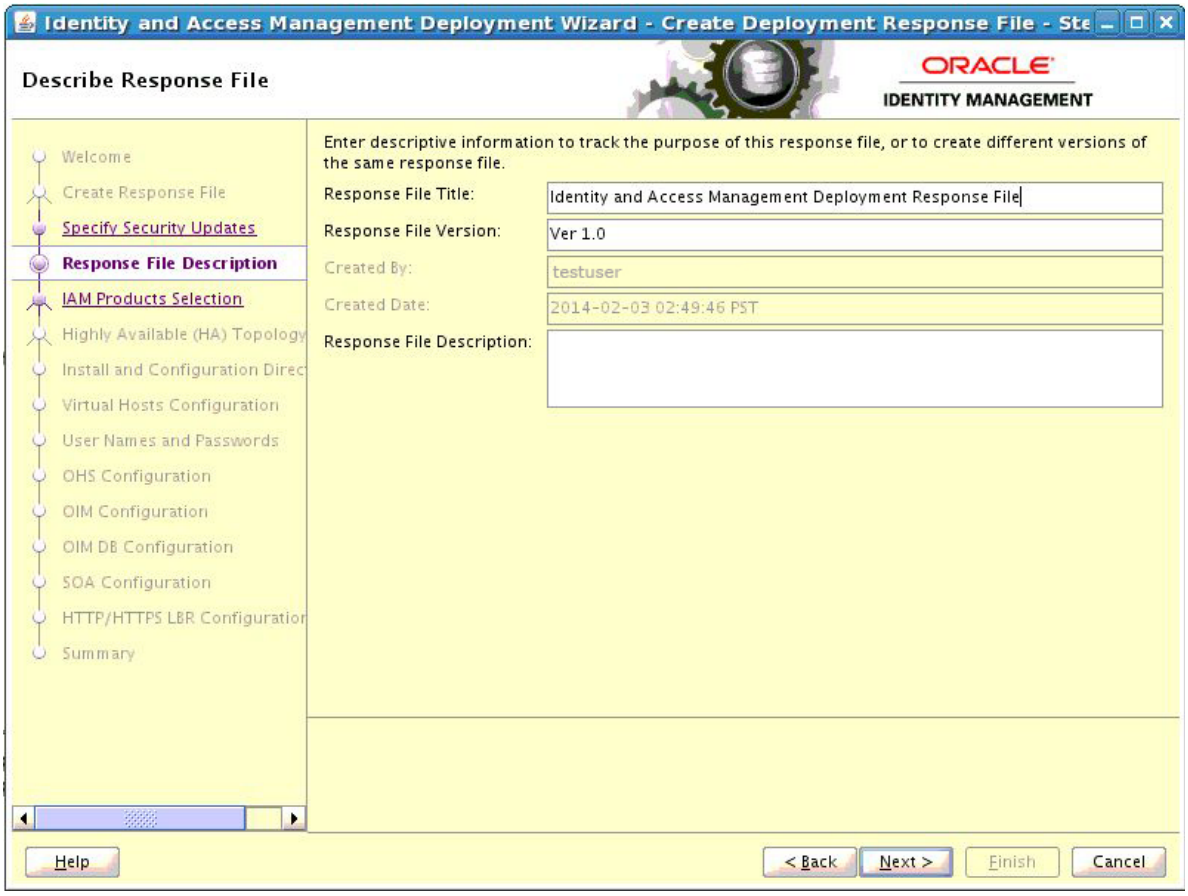


Click **Next** to continue.

4.4.2.5 Describe Response File

Specify descriptive information to identify the response file. The information entered on this screen is metadata information. This information can be used to uniquely identify a response file if multiple response files are created.

- **Response File Title**: The Oracle Identity and Access Management Deployment Wizard provides the default title `Oracle Identity and Access Management Deployment Response File`. You can change this.
- **Response File Version**: The Oracle Identity and Access Management Deployment Wizard provides a default value, which you can change. You can use this to keep track of different file versions.
- **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.



Click **Next** to continue.

4.4.2.6 Select IAM Products

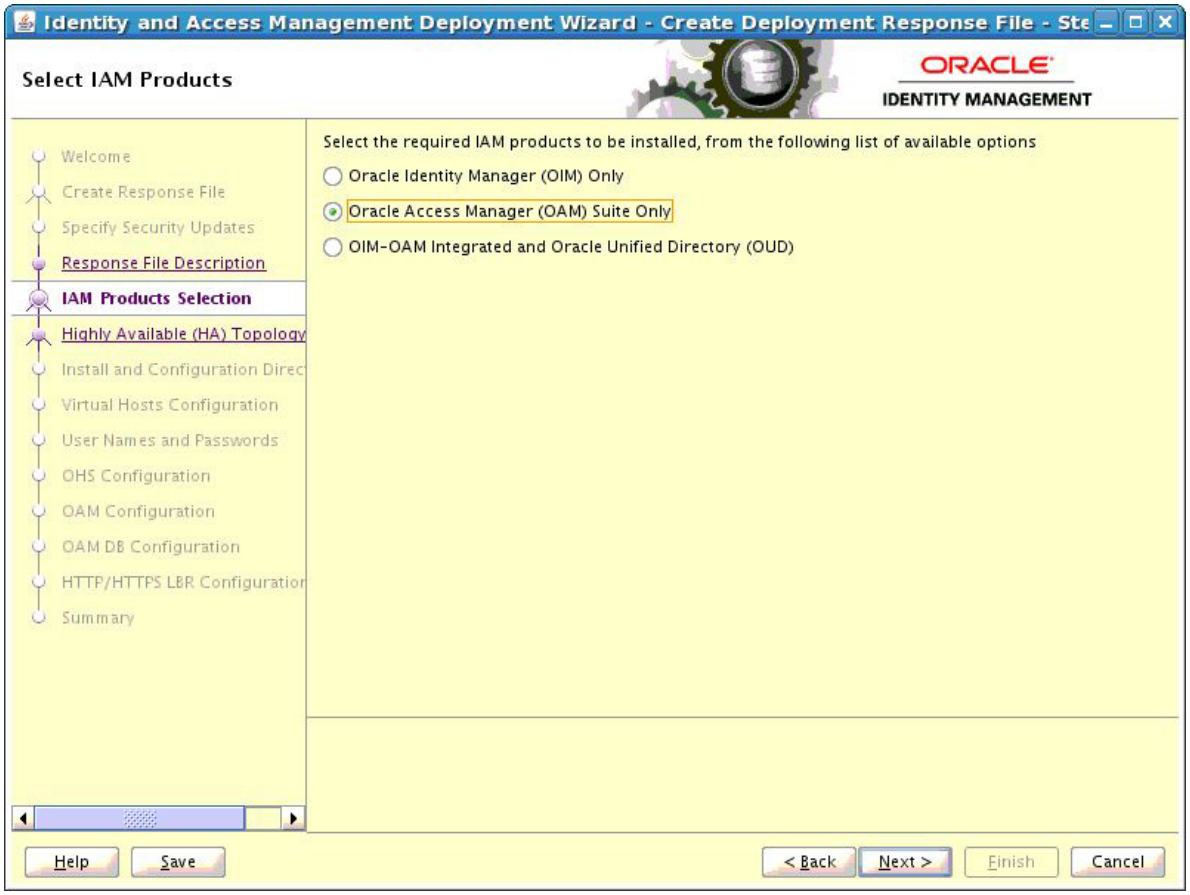
On the Select IAM Products screen, select the type of deployment that you would like to perform. The following options are available:

- **Oracle Identity Manager (OIM) Only**: Select this option to install and configure Oracle Identity Manager and SOA with Oracle HTTP Server.
- **Oracle Access Manager (OAM) Suite Only**: Select this option to install and configure Oracle Access Management suite with Webgate and Oracle HTTP Server.
- **OIM-OAM Integrated and Oracle Unified Directory (OUD)**: Select this option to install and configure the following products:
  - Oracle Identity Manager
  - Oracle SOA
  - Oracle Access Management
  - Oracle Unified Directory
  - Oracle HTTP Server
  - Webgate

Note: If you want to deploy a multiple host topology using the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option, then do not use this guide. This guide covers only the following HA deployments:

- **Oracle Identity Manager (OIM) Only**
- **Oracle Access Manager (OAM) Suite Only**

For performing an HA deployment using you using the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option, you must refer to *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.



Note: After you select IAM components that 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, you must cancel this wizard, and restart the Oracle Identity and Access Management Deployment Wizard.

Click **Next** to continue.

4.4.2.7 Select Topology

Use the Select Topology screen to select configuration options and provide information about hosts and products.

- **Single Node**: Select this option to deploy a simple, single host topology.
  - **Host Name**: Specify the host where you want to deploy Identity and Access Management, as a fully-qualified host name.
- **Highly Available (HA)**: This option enables you to deploy a multiple host topology. Select this option to perform an HA deployment.

  You must provide the following information:

  Note: All host names must be fully qualified.

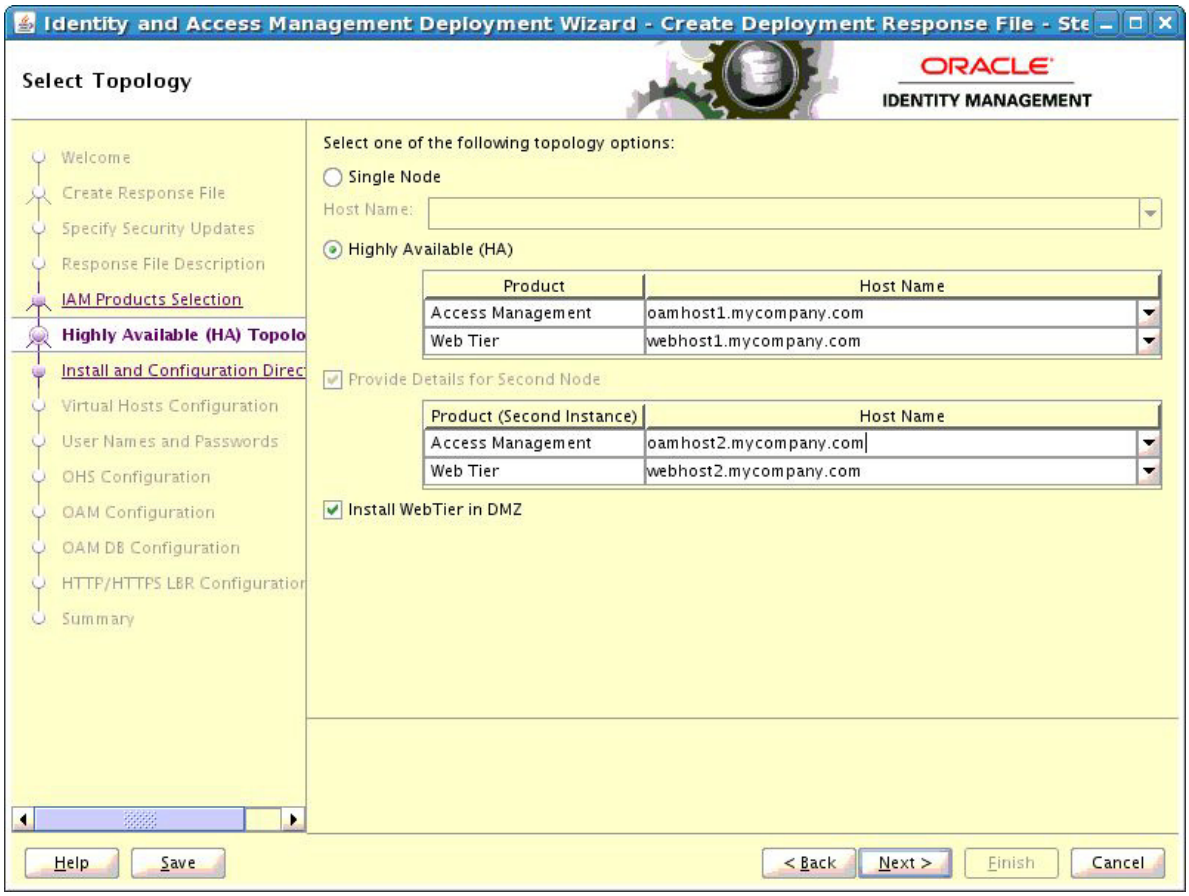
  The products that are listed under the Product column depends on the option that you selected on the "Select IAM Products" screen.

  - **Access Management**: Specify the fully qualified host name which will be running Oracle Access Management. For example, `OAMHOST1.mycompany.com`
  - **Web Tier**: Specify the fully qualified host name which will be running the Oracle HTTP server and WebGate. For example, `WEBHOST1.mycompany.com`

  Ensure **Provide Details for Second Node** is selected, then enter the following information:

  - **Access Management**: Specify the fully qualified host name which will be running the second instance of Oracle Access Management. For example, `OAMHOST2.mycompany.com`
  - **Web Tier**: Specify the fully qualified host name which will be running the second instance of Oracle HTTP server and WebGate. For example, `WEBHOST2.mycompany.com`

  Note: After you select the topology option, do not click the **Back** button in the subsequent screens to modify your topology options. If you need to make any modification in the previous screens, you must cancel this wizard, and restart the Oracle Identity and Access Management Deployment Wizard.



Click **Next** to continue.

4.4.2.8 Select Installation and Configuration Locations

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

- **Lifecycle Management Store Location**: This is a location for storing data to support lifecycle management, for example: `/u01/lcm` (*LCM_HOME*)

  Log files are present under the logs directory in *LCM_HOME*. On Linux, this is located at *LCM_HOME*`/provisioning/logs`.

  > **Note:** You should mount the *LCM_HOME* directory on every host for the duration of Identity and Access Management Deployment. If you have done this, select the **Mounted on Web hosts** option.
  >
  > If, however, you cannot mount the directory for the duration of provisioning, you can still perform deployment, but you must also perform some manual steps. See Section 5.3, "Deploying Identity and Access Management Without a Common LCM_HOME" for details.

- **Mounted on Web hosts**: If you have mounted your *LCM_HOME* directory on your web hosts then, select Mounted on Web hosts.
- **Software Repository Location**: This is the location of the Deployment repository, for example: `/u01/lcm/Repository`

- **Software Installation Location**: This is the location on shared storage under where you want the Middleware Home to be placed, for example: `/u01/oracle`

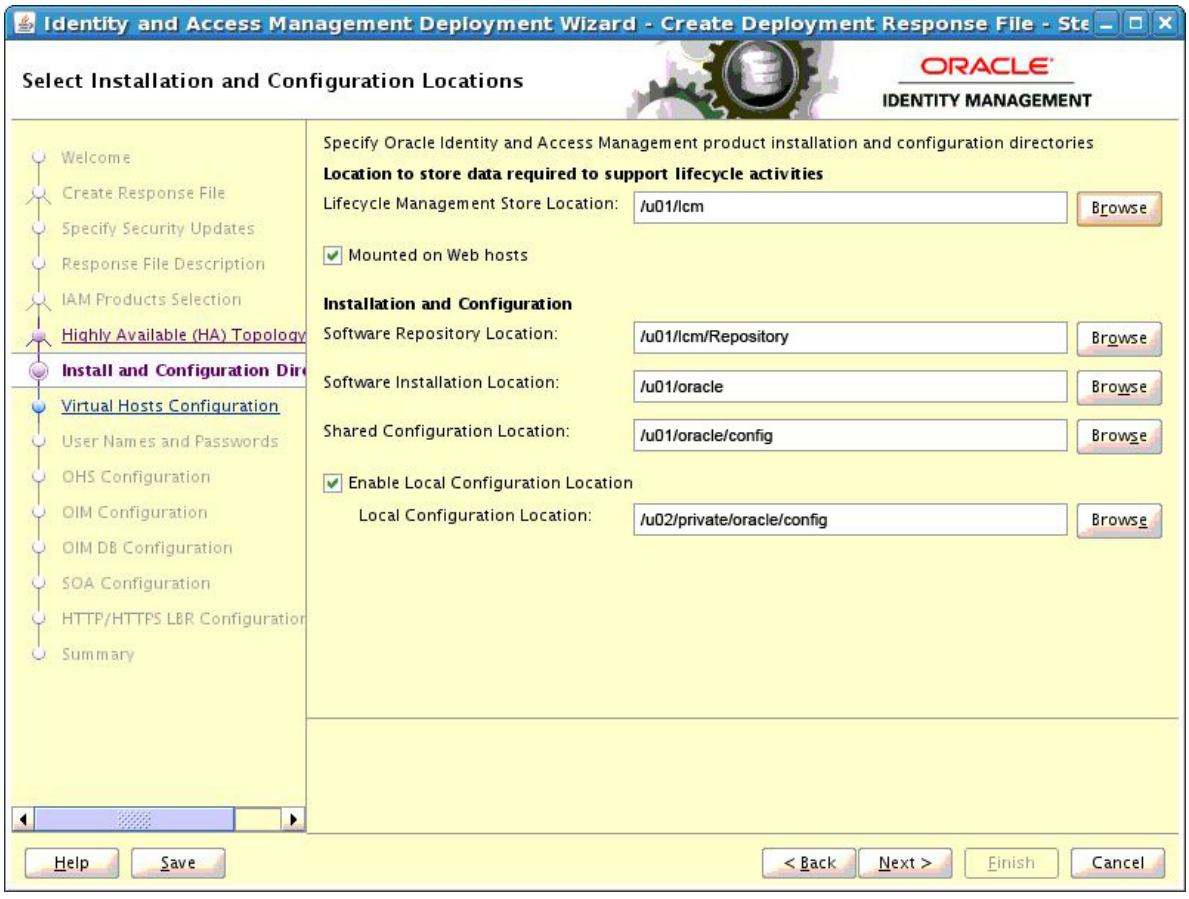
  Ensure that this directory path is 45 characters or fewer in length. A longer pathname can cause errors during Oracle Identity and Access Management deployment. See Section 8.2.1, "Null Error Occurs When WebLogic Patches Are Applied."

- **Shared Configuration Location**: Specify the location of shared configuration, for example: `/u01/oracle/config` (*`SHARED_CONFIG_DIR`*).

- **Enable Local Configuration Location**: Select this option to enable local configuration.

- **Local Configuration Location**: This is the location on local storage where the OAM managed servers, and the OHS instances are stored, for example: `/u02/private/oracle/config`.

Note: The Identity and Access Management process requires that you use the same Deployment profile on all hosts in the deployment. Therefore, the locations you enter on this screen must be consistent across all hosts.



Click **Next** to continue.

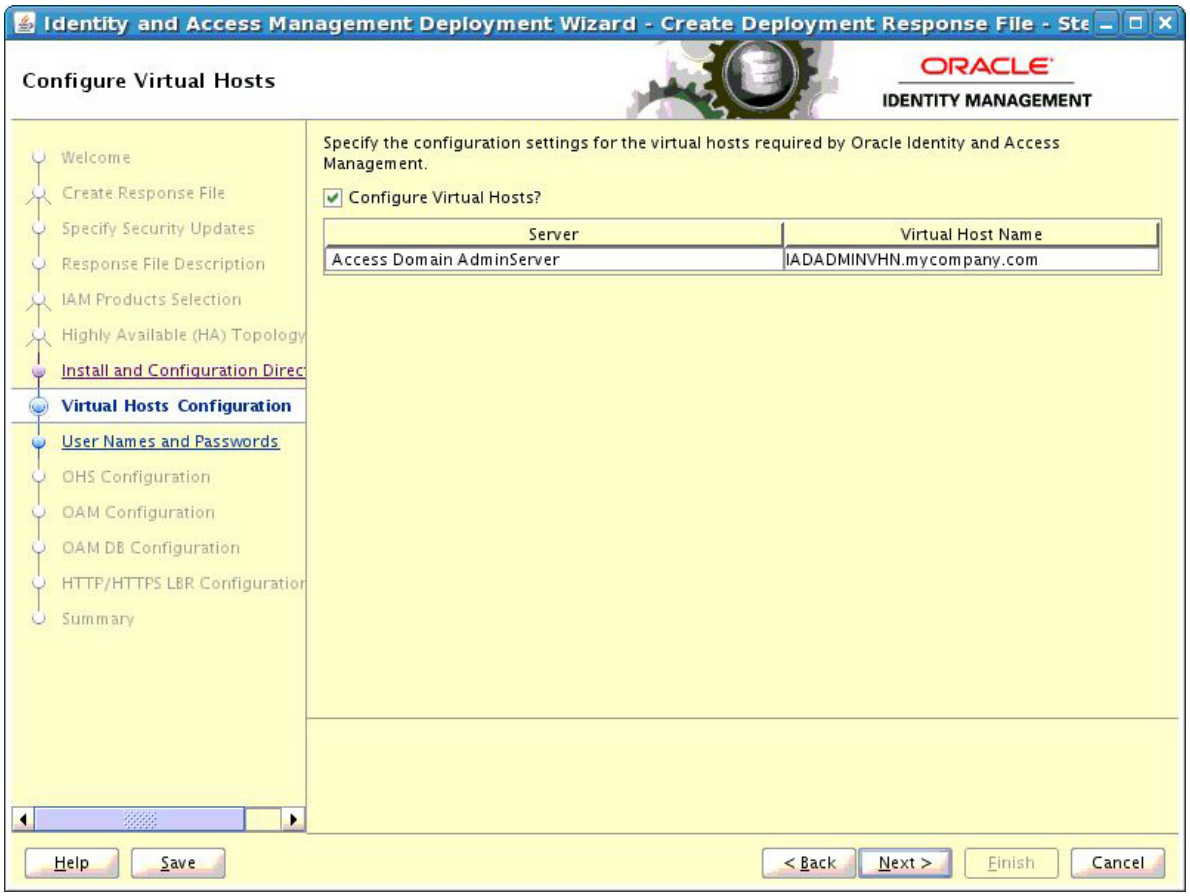
4.4.2.9 Configure Virtual Hosts

If you want to configure virtual hosts, then on the Configure Virtual Hosts screen, select the **Configure Virtual Hosts** check box, and provide the virtual host names for the servers listed on the screen.

For the Oracle Access Manager (OAM) Suite Only topology, you can provide a virtual host name for the Administration Server. The virtual host name should be resolved either through DNS or through the `/etc/hosts` file.

Enter the **Virtual Host Name** for each **Server** in the topology, for example:

Access Domain AdminServer: `IADADMINVHN.mycompany.com`



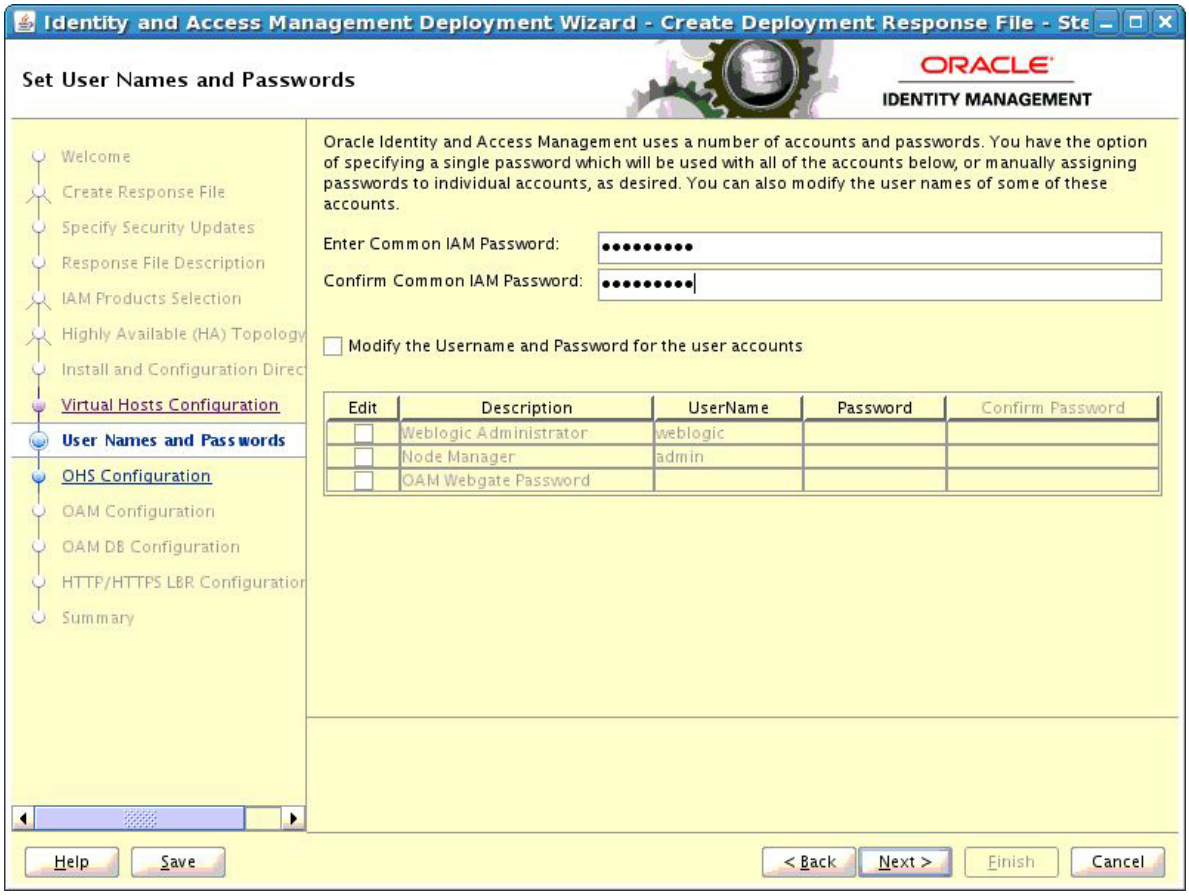
Click **Next**.

4.4.2.10 Set User Names and Passwords

The Set User Names and Passwords screen shows the users that will be created during the deployment process. You can either set a common password for all of the user accounts listed, or set individual passwords as required for each of the accounts. It is also possible to change some of the default usernames that are created, if desired.

- **Enter Common IAM Password**: Enter a common IAM password. This is the default password that will be used by all accounts unless overriden on an account by account basis.
- **Confirm Common IAM Password**: Re-enter the password.

- If you want to override the default usernames and common password, then select the **Modify the Username and Password for the user accounts** option. Select **Edit** next to the account you wish to modify, and override the Username and Password as desired.



Click **Next** to continue.

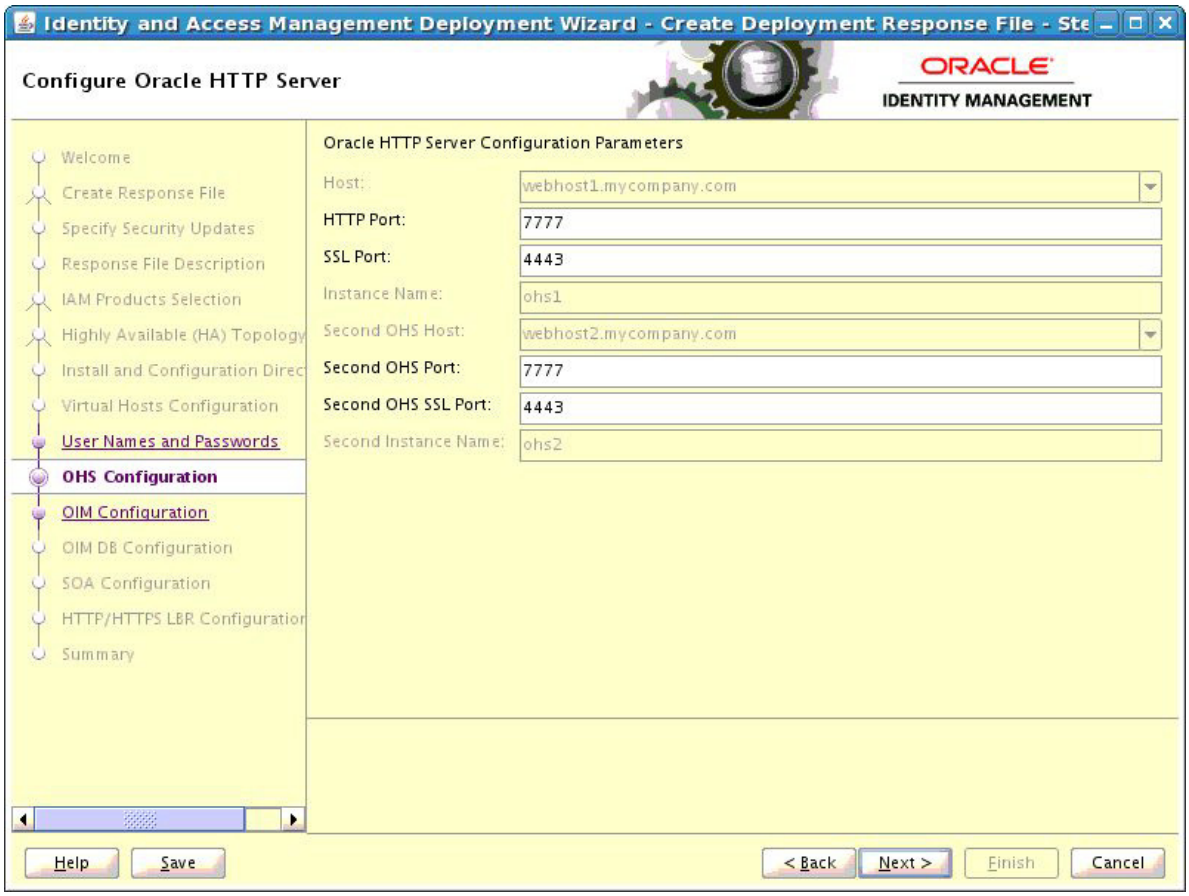
4.4.2.11 Configure Oracle HTTP Server

Use the Configure Oracle HTTP Server screen to change the installation ports used for Oracle HTTP Server (OHS).

Oracle HTTP Server Configuration Parameters

- **Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
- **HTTP Port**: Specify the non-SSL port number to be used for the Oracle HTTP Server.
- **SSL Port**: Specify the SSL port number to be used for the Oracle HTTP Server.
- **Instance Name**: This field is purely informational. It displays the instance name of the Oracle HTTP Server.
- **Second OHS Host**: This field is purely informational. The value is determined by the host entered in the Select Topology screen.
- **Second OHS Port**: Specify the non-SSL port number to be used for the second instance of Oracle HTTP Server.

- **Second OHS SSL Port**: Specify the SSL port number to be used for the second instance of Oracle HTTP Server.
- **Second Instance Name**: This field is purely informational. It displays the second instance name of the Oracle HTTP Server.

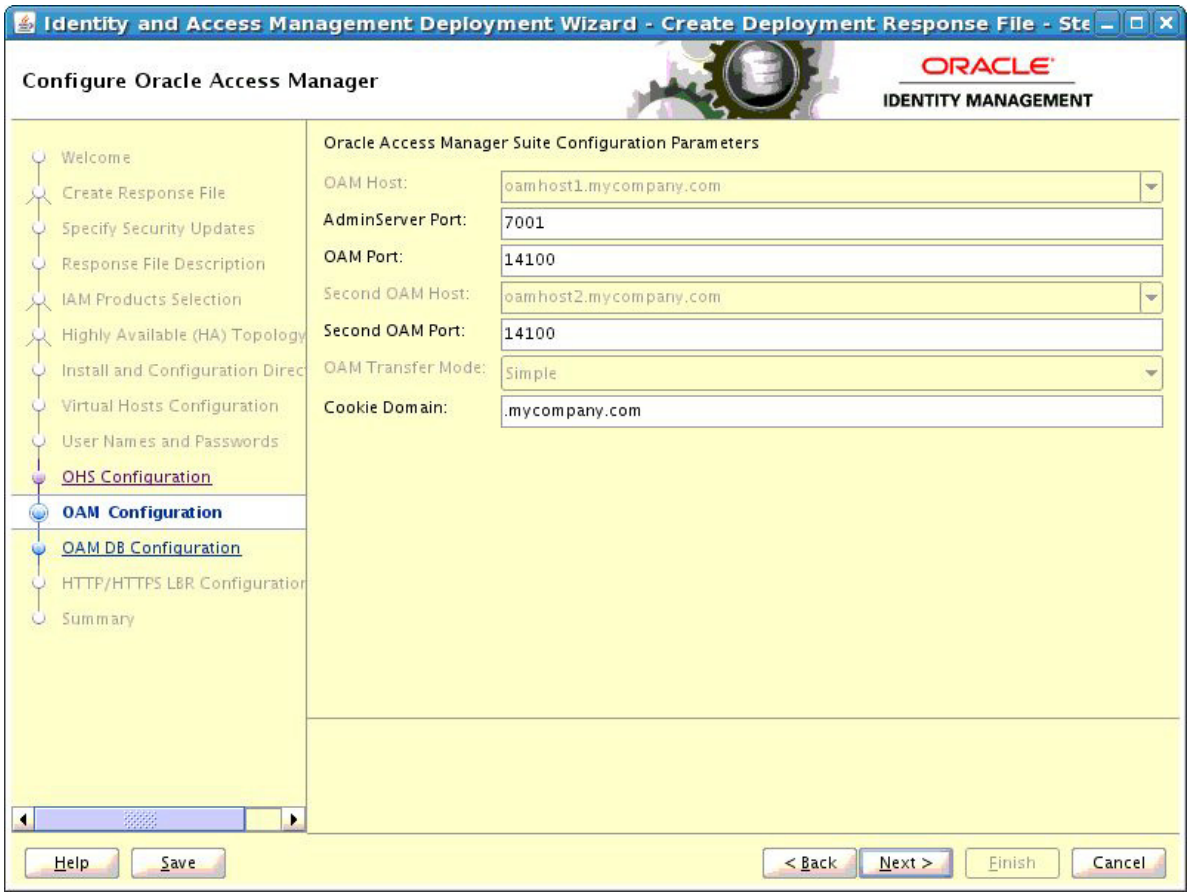


Click **Next** to continue.

4.4.2.12 Configure Oracle Access Manager

Use the Configure Oracle Access Manager screen to select installation options for Oracle Access Management suite.

- **OAM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology.
- **Admin Server Port**: The Port that the IAMAccessDomain Admin Server will use, for example: `7001`
- **OAM Port**: Specify the port number to be used by the first instance of OAM Managed Server, for example: `14100`
- **Second OAM Host**: This field is purely informational. The value is determined by the host entered in the Select Topology.
- **Second OAM Port**: Specify the port number to be used by the second instance of OAM Managed Server, for example: `14100`
- **OAM Transfer Mode**: This field is purely informational.
- **Cookie Domain**: Specify the cookie domain. For example: `.mycompany.com`



Click **Next**.

4.4.2.13 Configure Oracle Access Manager Database

Use the Configure Oracle Access Manager Database screen to enter information about the Database that contains the schemas for Oracle Access Manager.

- **Schema Prefix**: Specify the prefix that you want to use for the OAM schema. The schema prefix should be the same as the one that you provided when running the RCU.

  The default value of this field is `DEV`. This value can be edited.

- **Schema User Name**: This field specifies the name of the schema user.

  The value of this field depends on the **Schema Prefix** value. This field takes the value of **Schema Prefix** and adds an OAM suffix to it. For example, `DEV_OAM`.

- **Service Name**: Specify the service name of the database service, for example: `oamdb.mycompany.com`

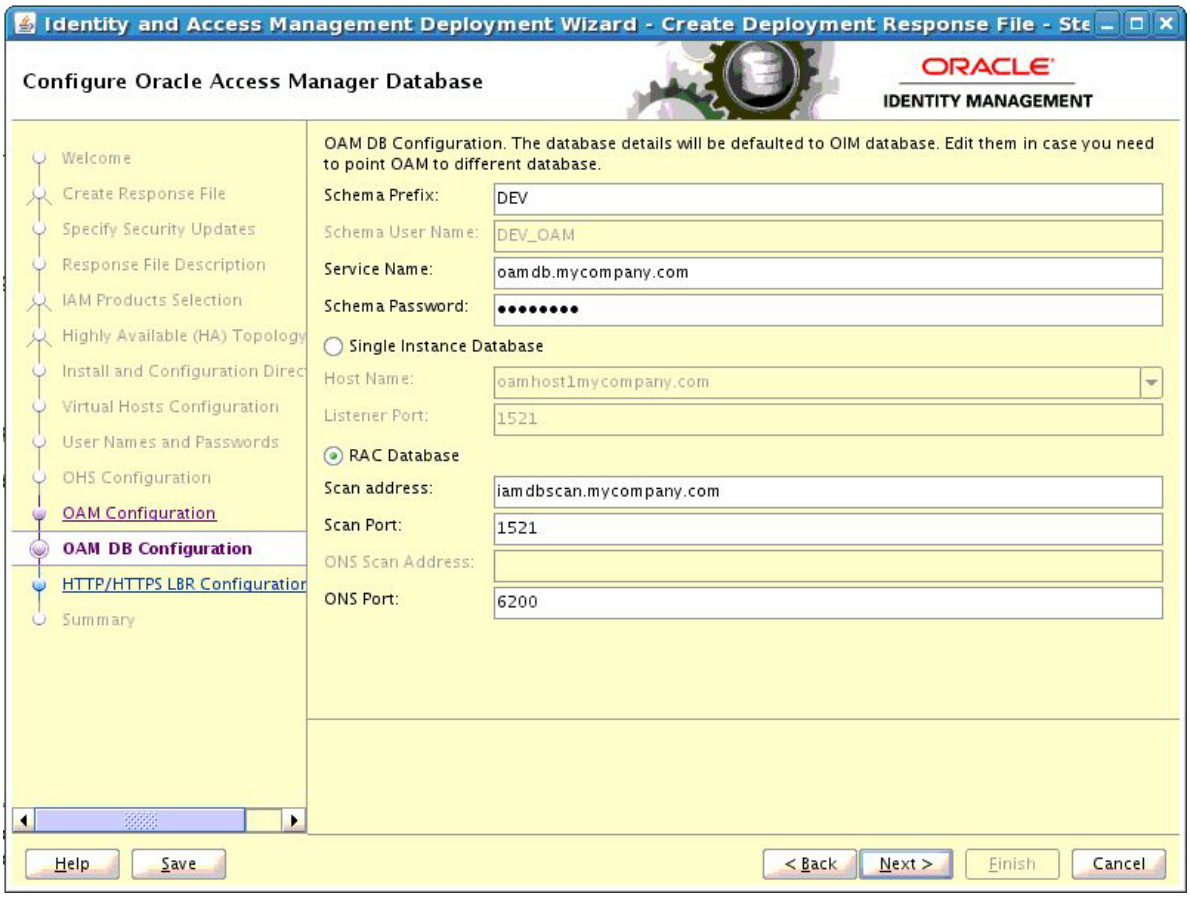
- **Schema Password**: Specify the password you used when creating the Oracle Access Manager schema using the Oracle Identity and Access Management RCU.

- **Single DB**: Select if you are using a single Oracle Database.
  - **Host VIP Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.

- **RAC DB**: Select if you are using an Oracle RAC Database.

- **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com`.
- **Scan Port**: Enter the port used by the Grid Infrastructure Listener, for example: `1521`.
- **ONS Scan Address**: Defaults to the scan address.
- **ONS Port**: Determine the ONS port by using the RAC `srvctl` command on the Oracle Database server, as shown in the following example:

```
srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```



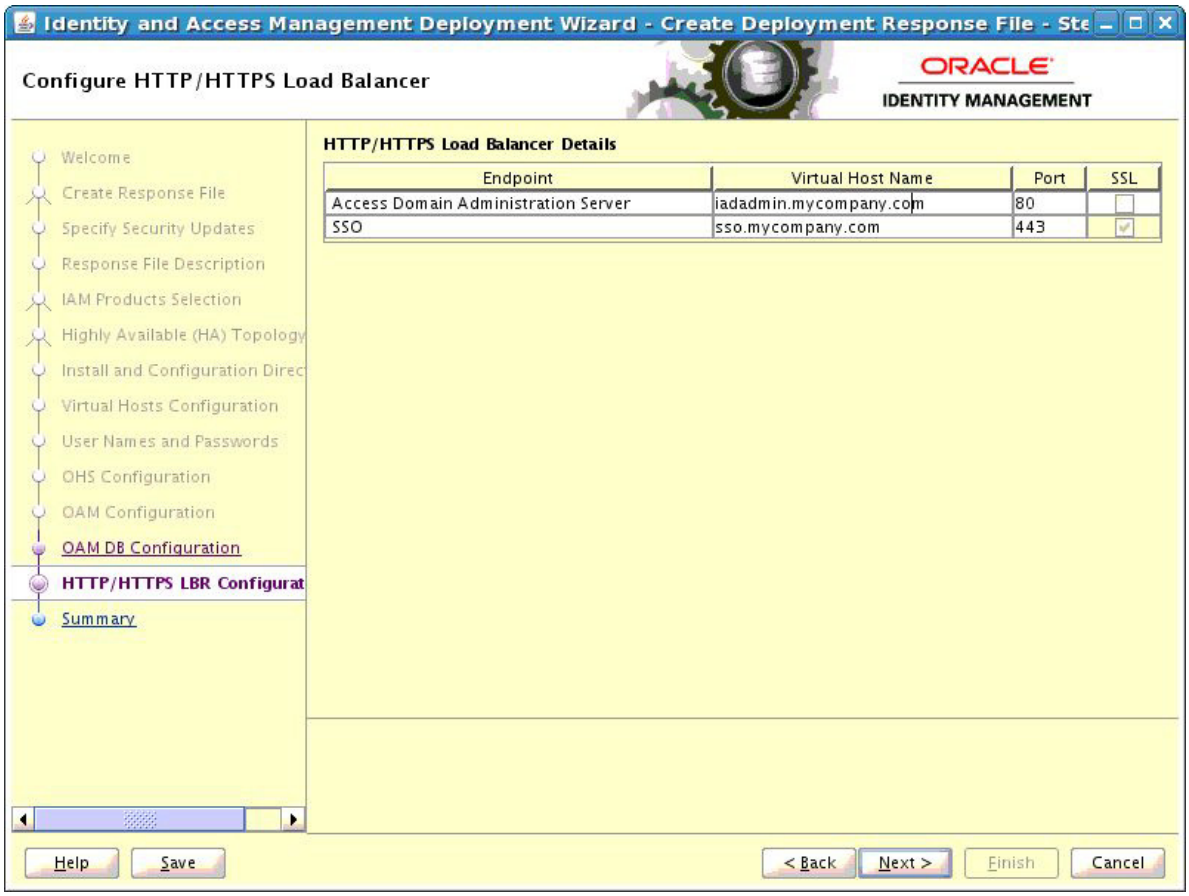
Click **Next** to continue.

4.4.2.14 Configure HTTP/HTTPS Load Balancer

On the HTTP/HTTPS Load Balancer screen, enter details about your load balancer virtual hosts.

Under **HTTP/HTTPS Load Balancer Details**, enter the **Virtual Host Name** and **Port** for each **Endpoint**.

- **Access Domain Administration Server**: The Load Balancer end point used to access the IAMAccessDomain Administration functions, for example: `iadadmin.mycompany.com`, Port `80`, Not SSL
- **SSO**: This is the main application entry point, for example: `sso.mycompany.com`, Port `443`

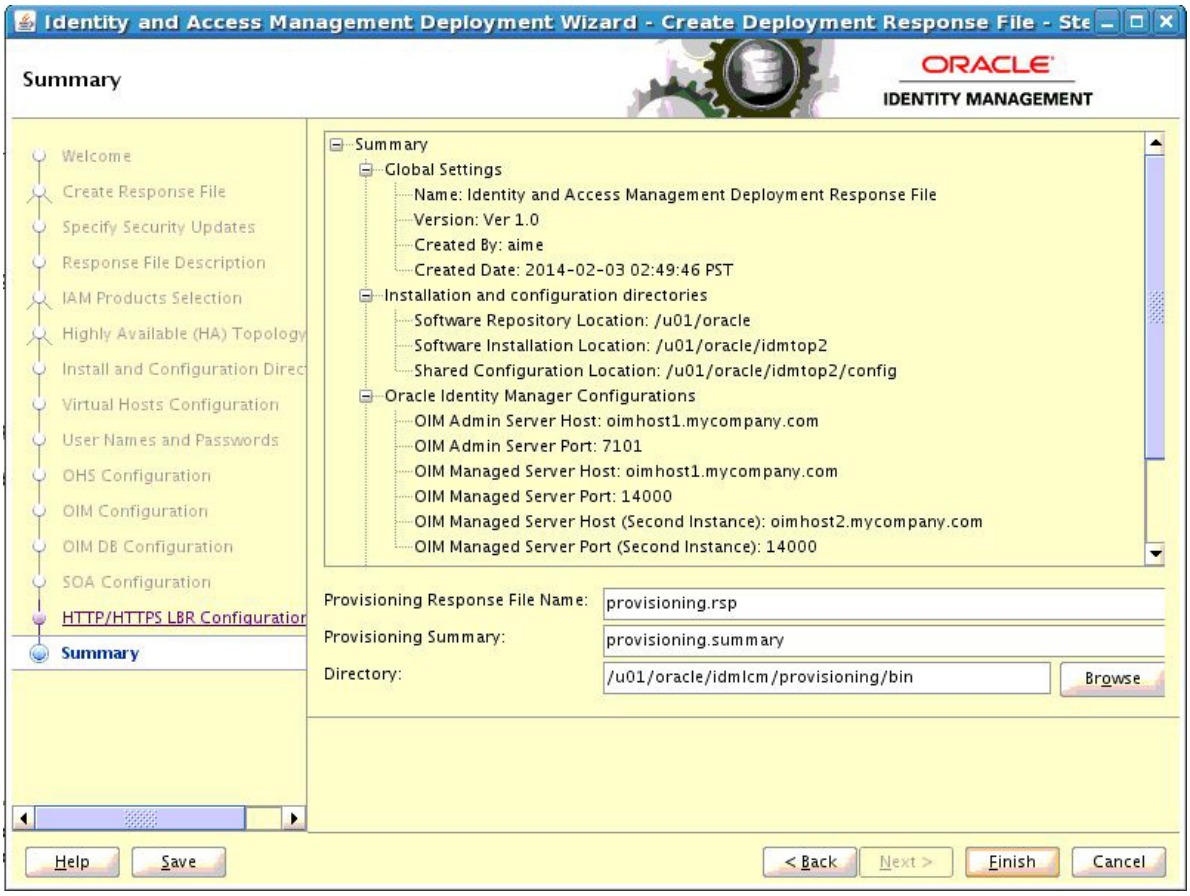


Click **Next**.

4.4.2.15 Summary

Use the Summary screen to view a summary of your selections and enter details about the response file.

- **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.



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 Copying Required Artifacts to DMZ Hosts

Complete this task only if you have installed web tier in the DMZ.

The process described in this chapter creates a deployment response file in the directory you specified on the Summary screen. When a deployment response file is created (for example, `provisioning.rsp`), an additional folder named *responsefilename*_`data` is created. For example, `provisioning_data`. This folder contains `cwallet.sso`, which has encryption and decryption information.

The deployment response file and the folder containing `cwallet.sso` must be available to each host in the topology. If you have a deployment directory shared across all hosts in the topology, then the required files are automatically available. If, however, you have not shared your deployment directory, you must manually copy

the deployment response file (`provisioning.rsp`) and the folder containing `cwallet.sso` (`provisioning_data`) to the same location on the DMZ hosts, WEBHOST1, and WEBHOST2.

Note: If the deployment response file and the folder containing cwallet.sso are not copied to the DMZ hosts, the deployment process may fail in the preverify phase.

5

Performing Oracle Identity and Access Management Deployment

After you create the deployment response file, you 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:

5.1 Performing Deployment on a Single-Node

Single-node deployment is accomplished by using either the command line or the Oracle Identity and Access Management Deployment Wizard.

> **Note:** You must reboot the host before performing Oracle Identity and Access Management deployment.

This section contains the following topics:

5.1.1 Introduction to the Deployment Process

This section contains the following topics:

5.1.1.1 Oracle Identity and Access Management Deployment Stages

After you create the deployment response file, you use it to deploy the Oracle Identity and Access Management environment.

There are eight stages to deployment. These stages must be run in the following order:

1. **preverify**
2. **install**
3. **preconfigure**
4. **configure**
5. **configure-secondary**
6. **postconfigure**
7. **startup**
8. **validate**

> **Note:** Each new phase must run sequentially; that is, each stage must be completed before the next stage can begin. Failure of a stage will necessitate a cleanup and restart.

5.1.1.2 Tasks Performed During Deployment Stages

The tasks that are performed in each stage of Deployment, depend on the option that you selected on the **Select IAM Products** screen. This screen appears when you create the deployment response file using the Oracle Identity and Access Management Deployment Wizard.

Based on the products that you selected for Deployment, refer to one of the sections below:

- Oracle Identity Manager (OIM) Only
- Oracle Access Manager (OAM) Suite Only
- OIM-OAM Integrated and Oracle Unified Directory (OUD)

Oracle Identity Manager (OIM) Only

Table 5–1 describes the order of execution of the Deployment stages, and the tasks that are performed in each stage for the **Oracle Identity Manager (OIM) Only** option.

Table 5–1 Tasks Performed for Oracle Identity Manager (OIM) Only

Order of Execution	Stage	Tasks Performed
1.	**preverify**	Checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.
2.	**install**	Installs all of the software and related patches present in Oracle Identity and Access Management deployment repository.
3.	**preconfigure**	▪ Creates the WebLogic Domain and extends it to all the necessary components ▪ Creates OHS instance

Table 5–1 (Cont.) Tasks Performed for Oracle Identity Manager (OIM) Only

Order of Execution	Stage	Tasks Performed
4.	**configure**	■ Starts managed servers as necessary ■ Configures OIM
5.	**configure-secondary**	■ Integrates Weblogic Domain with Webtier ■ Registers Webtier with domain
6.	**postconfigure**	Configures UMS Mail Server
7.	**startup**	Starts up all components in the topology
8.	**validate**	Verifies the deployed environment.

Oracle Access Manager (OAM) Suite Only

Table 5–2 describes the order of execution of the Deployment stages, and the tasks that are performed in each stage for the **Oracle Access Manager (OAM) Suite Only** option.

Table 5–2 Tasks Performed for Oracle Access Manager (OAM) Suite Only

Order of Execution	Stage	Tasks Performed
1.	**preverify**	Checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.
2.	**install**	Installs all of the software and related patches present in Oracle Identity and Access Management deployment repository.
3.	**preconfigure**	■ Creates the WebLogic Domain and extends it to all the necessary components ■ Creates OHS instance
4.	**configure**	■ Starts managed servers as necessary ■ Configures OAM to enable SSO.
5.	**configure-secondary**	■ Integrates Weblogic Domain with Webtier ■ Registers Webtier with domain
6.	**postconfigure**	■ Generates OAM Keystore ■ Configures Webgates
7.	**startup**	Starts up all components in the topology
8.	**validate**	Verifies the deployed environment.

OIM-OAM Integrated and Oracle Unified Directory (OUD)

Table 5–3 describes the order of execution of the Deployment stages, and the tasks that are performed in each stage for the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option.

Table 5–3 Tasks Performed for OIM-OAM Integrated and Oracle Unified Directory (OUD)

Order of Execution	Stage	Tasks Performed
1.	**preverify**	Checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.

Table 5–3 (Cont.) Tasks Performed for OIM-OAM Integrated and Oracle Unified Directory

Order of Execution	Stage	Tasks Performed
2.	**install**	Installs all of the software and related patches present in Oracle Identity and Access Management deployment repository.
3.	**preconfigure**	■ Creates OUD and seeds it with Users/Groups. ■ SSL Enable OUD ■ Creates the WebLogic Domain and extends it to all the necessary components ■ Creates OHS instance
4.	**configure**	■ Starts managed servers as necessary ■ Configures OIM ■ Associates OAM with OUD
5.	**configure-secondary**	■ Integrates Weblogic Domain with Webtier ■ Registers Webtier with domain ■ Integrates OAM and OIM
6.	**postconfigure**	■ Runs OIM Reconciliation ■ Configures UMS Mail Server ■ Generates OAM Keystore ■ Configures Webgates
7.	**startup**	Starts up all components in the topology
8.	**validate**	Verifies the deployed environment.

5.1.2 Performing Deployment by Running the Deployment Tool

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.

Before running the deployment tool, ensure that the environment variable `JAVA_HOME` is set to *`REPOS_HOME`*`/jdk6`.

The command syntax for the deployment tool on UNIX is:

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

Where:

`RESPONSE_FILE` is the complete path to the location of the deployment response file. You specified the file name and directory on the Summary Page when you ran the wizard to create the deployment response file. The default value is *`IDMLCM_HOME`*`/provisioning/bin/provisioning.rsp` on UNIX.

`STAGE` is one of the stages listed in Section 5.1.1.1, "Oracle Identity and Access Management Deployment Stages."

Example:

```
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
```

5.1.3 Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard

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

1. Before running the Oracle Identity and Access Management Deployment Wizard, ensure that the environment variable `JAVA_HOME` is set to *`REPOS_HOME`*`/jdk6`.
2. Start the Oracle Identity and Access Management Deployment Wizard, as follows:

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

The Welcome screen is displayed. Click **Next**, and proceed as described in the following sections.

Note: In the Prerequisite Checks, Installation, Preconfigure, Configure, Configure Secondary, Postconfigure, and Startup pages, the Status of each build is indicated by one of these icons:

- **Block**: Processing has not yet started for the named phase.
- **Clock**: Performing the build for a phase.
- **Check mark**: The build was completed successfully.
- **x** mark: The build has failed for this phase. You must correct the errors before you can continue.

Click **x** to display information about failures. Click a build **Log** file to see details specific to that build.

In case of errors, you must manually clean up everything. Kill all running processes, delete the directories, rerun RCU, and start over from the beginning. For more information, see Section 8.1.2, "Recovering From Oracle Identity and Access Management Deployment Failure".

- Section 5.1.3.1, "Choose IAM Installation Options"

5.1.3.1 Choose IAM Installation Options

Select **Deploy an Identity and Access Management Environment** to use an existing deployment response file to deploy the environment.

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."

Click **Next** to continue.

5.1.3.2 Describe Response File

Use the Describe Response File screen to review the information about the response file, that you had provided when creating the Deployment Profile.

For more information, see Section 4.4.1.5, "Describe Response File".

5.1.3.3 Select Installation and Configuration Locations

Use the Select Installation and Configuration Locations screen to 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 Section 4.4.1.8, "Select Installation and Configuration Locations".

5.1.3.4 Review Deployment Configuration

The Review Deployment Configuration screen enables you to select configurations you want to review. This is optional. 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**

Click **Next** to continue.

5.1.3.5 Summary

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

Review the information displayed to ensure that the installation details are what you intend.

Click **Next** to continue.

5.1.3.6 Prerequisite Checks

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next** to continue.

5.1.3.7 Installation

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next** to proceed.

5.1.3.8 Preconfigure

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard starts the configure phase and displays the Configure screen.

5.1.3.9 Configure

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard starts the Configure-secondary phase and displays the Configure Secondary screen.

5.1.3.10 Configure Secondary

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard starts the Postconfigure phase and displays the Postconfigure screen.

5.1.3.11 Postconfigure

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard starts the Startup phase and displays the Startup screen.

5.1.3.12 Startup

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard starts the Validate phase and displays the Validation screen.

5.1.3.13 Validation

For information about the tasks that are performed during this stage, refer to Section 5.1.1.2, "Tasks Performed During Deployment Stages".

See the note at the beginning of Section 5.1.3, "Performing Deployment Using the Oracle Identity and Access Management Deployment Wizard" for information about viewing build status on this page.

Click **Next**. The Oracle Identity and Access Management Deployment Wizard displays the Install Complete screen.

5.1.3.14 Install Complete

This screen appears after deployment has completed successfully. It shows a summary of the products that have been installed.

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

5.2 Performing Deployment on Multiple Hosts Using the Command Line Deployment Tool

This section describes the procedure for performing deployment on multiple hosts. It contains the following sections:

5.2.1 Introduction to the Deployment Process

This section contains the following topics:

5.2.1.1 Deployment Stages

There are eight stages to deployment. These stages must be run in the following sequence:

1. `preverify`
2. `install`
3. `preconfigure`
4. `configure`-secondary
5. `postconfigure`
6. `startup`
7. `validate`

Each new phase must run sequentially; that is, each stage must be completed before the next stage can begin. Stage failures require a cleanup and restart.

5.2.1.2 Tasks Performed During OIM-Only Deployment

Table 5–4 describes the order of execution of the deployment stages, and the tasks that are performed in each stage for the Oracle Identity Manager (OIM) Only option.

Table 5–4 Deployment Stages (OIM-Only)

Order of Execution	Stage	Tasks Performed	Sequence
1	preverify	Checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.	In the `preverify` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.

Table 5–4 (Cont.) Deployment Stages (OIM-Only)

Order of Execution	Stage	Tasks Performed	Sequence
2	install	Installs all of the software and related patches present in Oracle Identity and Access Management deployment repository.	In the `install` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
3	preconfigure	Creates the WebLogic Domain and extends it to all the necessary components and creates OHS instance.	In the `preconfigure` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
4	configure	Starts managed servers, as necessary. Configures OIM.	In the `configure` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
5	configure-secondary	Integrates Weblogic domains with the Web tier, and registers the Web tier with the domains.	In the `configure--secondary` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.

Table 5–4 (Cont.) Deployment Stages (OIM-Only)

Order of Execution	Stage	Tasks Performed	Sequence
6	postconfigure	Configures UMS Mail Server.	In the `postconfigure` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
7	startup	Starts up all components in the topology.	In the `startup` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
8	validate	Verifies the deployed environment.	In the `validate` stage, run the deployment tool on the command line on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.

5.2.1.3 Tasks Performed During OAM-Only Deployment

Table 5–5 describes the order of execution of the deployment stages, and the tasks that are performed in each stage for the Oracle Access Management Suite (OAM-Only) option.

Table 5–5 Deployment Stages (OAM-Only)

Order of Execution	Stage	Tasks Performed	Sequence
1	preverify	Checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.	In the `preverify` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
2	install	Installs all of the software and related patches present in Oracle Identity and Access Management deployment repository.	In the `install` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
3	preconfigure	Creates the WebLogic Domain and extends it to all the necessary components and creates OHS instance.	In the `preconfigure` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
4	configure	Starts managed servers, as necessary. Configures OAM to enable SSO.	In the `configure` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.

Table 5–5 (Cont.) Deployment Stages (OAM-Only)

Order of Execution	Stage	Tasks Performed	Sequence
5	configure-secondary	Integrates Weblogic domains with the Web tier, and registers the Web tier with the domains.	In the `configure--secondary` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
6	postconfigure	Generates OAM keystore and configures WebGate agents.	In the `postconfigure` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
7	startup	Starts up all components in the topology.	In the `startup` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.
8	validate	Verifies the deployed environment.	In the `validate` stage, run the deployment tool on the command line on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Follow the same sequence and one by one. Do not run them in parallel.

5.2.2 Deployment Procedure

The following sections describe the procedure for performing Deployment.

Note: Before you start the deployment process, reboot all hosts.

- Section 5.2.2.1, "Running the Deployment Commands"
- Section 5.2.2.2, "Creating Backups"

5.2.2.1 Running the Deployment Commands

After creating the required deployment response profile based on your installation scenario, you must perform deployment by running the command `runIAMDeployment.sh` a number of times on each host in the topology.

Before embarking on the Deployment process, read this entire section. There are extra steps detailed below which must be performed during the process.

You must run each command on each host in the topology before running the next command.

Before running the Deployment tool, set the following environment variable:

Set `JAVA_HOME` to: *`REPOS_HOME`*`/jdk6`

The commands you must run are:

```
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
```

> **Note:** Run same phase on each host, in order. Wait for a phase to finish before starting the same phase on the next host. You cannot run these phases in parallel. Repeat this for each phase.

5.2.2.2 Creating Backups

It is important that you take a backup of the file systems and databases at the following points:

1. Prior to starting Deployment.
2. At the end of the installation phase.
3. Upon completion of Deployment

It is not supported to restore a backup at any phase other than those three.

5.3 Deploying Identity and Access Management Without a Common LCM_HOME

The previous deployment instructions assume that the *LCM_HOME* directory is shared across every host in the topology for the duration of the deployment process.

If your organization does not permit this sharing, you can still run the deployment by making *LCM_HOME* available locally on every host. The following extra manual steps are required.

1. Create a local version of the *LCM_HOME* directory, including the software repository.
2. Copy the Deployment Response File, *responsefilename*_data folder, and Summary created in Section 4.4.2.15, "Summary" to the same location on each of the hosts.
3. If *LCM_HOME* is not mounted on WEBHOST1 and WEBHOST2, before execution of the postconfigure phase on WEBHOST1, copy *LCM_HOME*/keystores/webgate_artifacts from OAMHOST1 to WEBHOST1 and WEBHOST2

   LCM_HOME/keystores/webgate_artifacts is created after the configure phase on OAMHOST1.

5.4 Additional Information on Oracle HTTP Server Configuration Files

When you perform an Oracle Identity And Access Management deployment, Oracle HTTP Server is setup in the reverse proxy mode. The modules for Oracle HTTP Server are contained in files with a .conf extension. These files are located at:

config/instances/ohs1/config/OHS/ohs1/moduleconf

If you had selected the Enable Local Configuration Location option on the Select Installation and Configuration Locations screen when creating the deployment response file, then *config* is the local configuration location. If you had not selected the Enable Local Configuration Location option on the Select Installation and Configuration Locations screen when creating the deployment response file, then *config* is the location of shared configuration.

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:

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:

6.1 Post Deployment Tasks for Oracle Identity Manager

Complete the tasks described in the following sections:

6.1.1 Add an Oracle Identity Manager Property

As a workaround for a bug in the Oracle Identity and Access Management Deployment tools, you must add an Oracle Identity Manager property. Perform the following steps:

1. Log in to the WebLogic Console in the IAMGovernanceDomain by using the following URL:

   `http://IGDADMIN.mycompany.com/console`

   Log in as the user `weblogic`.
2. Navigate to **Environment -> Servers**.
3. Click **Lock and Edit**.
4. Click the managed server **WLS_OIM1**.
5. Click the **Server Start** subtab
6. Add the following to the **Arguments** field:

   ```
   -Djava.net.preferIPv4Stack=true
   ```
7. Click **Save**.
8. Repeat Steps 4-7 for the managed server **WLS_OIM2**.
9. Click **Activate Changes**.
10. Restart the managed WebLogic server.

6.1.2 Post-Deployment Steps for the E-mail Server Configuration

If you configured an e-mail server in Section 4.4.1.12, "Configure Oracle Identity Manager" and the mail server security is SSL, follow these additional steps:

1. Ensure that the proxy is set for the environment

   a. Stop Administration and Managed Server

   b. Back up the *IGD_MSERVER_HOME*/bin/setDomainEnv.sh

   c. Modify the *IGD_MSERVER_HOME*/bin/setDomainEnv.sh to include the proxy settings

   d. Include the following command as part of the environment setup in the setDomainEnv.sh file:

```
export PROXY_SETTINGS="-Dhttp.proxySet=true
 -Dhttp.proxyHost=www-proxy.mycompany.com -Dhttp.proxyPort=80
 -Dhttp.nonProxyHosts=localhost|$.mycompany.com|.mycompany.com|.mycompany.com"
```

   Example:

```
export JAVA_PROPERTIES
export PROXY_SETTINGS="-Dhttp.proxySet=true
 -Dhttp.proxyHost=www-proxy.mycompany.com -Dhttp.proxyPort=80
 -Dhttp.nonProxyHosts=localhost|${HOST}|*.mycompany.com"ARDIR="${WL_
HOME}/server/lib"
export ARDIR
```

2. Remove DemoTrust store references from SOA environment. This would run SOA in non-ssl mode.

   a. Modify the *IGD_MSERVER_HOME* to remove the DemoTrust references

   b. Remove the following references from setDomainEnv.sh:

```
-Djavax.net.ssl.trustStore=$<WL_HOME>/server/lib/DemoTrust.jks from EXTRA_JAVA_
PROPERTIES
```

   c. Restart the Administration server and the Managed servers.

6.2 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 selected the **Oracle Identity Manager (OIM) Only** option on the Select IAM Products screen when creating the deployment response file.

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

```
http://hostname:port/oamconsole
```

Note: If you have selected the **Oracle Access Manager (OAM) Suite Only** option on the Select IAM Products screen when creating the deployment response file, then use your WebLogic credentials to log in to the Oracle Access Manager Console.

If you have selected the **OIM-OAM Integrated and Oracle Unified Directory (OUD)** option on the Select IAM Products screen when creating the deployment response file, then use your oamAdminUser credentials to log in to the Oracle Access Manager Console.

2. In the **Access Manager** pane, click **Application Domains**.
3. A **Search Application Domains** tab opens. In the Name field, enter **IAM Suite**, and click **Search**.
4. In the **Search Results**, click **IAM Suite**.
5. Click the **Resources** tab.
6. Click **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 **Apply**.

6.3 Starting and Stopping Components

After the Identity and Access Management deployment is complete, it is important that various components of the deployment are started, stopped and restarted in the right order. The components can be started and stopped using a script or WLST commands. For more information, see section "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, "Validating the Administration Server"
- Section 7.2, "Validating the Access Manager Configuration"
- Section 7.3, "Validating Oracle Identity Manager"
- Section 7.4, "Validating SOA Instance from the WebTier"
- Section 7.5, "Validating WebGate and the Access Manager Single Sign-On Setup"

7.1 Validating the Administration Server

Validate the WebLogic Administration Server as follows:

- Section 7.1.1, "Verifying Connectivity"
- Section 7.1.2, "Validating Failover"

7.1.1 Verifying Connectivity

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

- Section 7.1.1.1, "Verifying Connectivity for Oracle Identity Manager"
- Section 7.1.1.2, "Verifying Connectivity for Oracle Access Management"

7.1.1.1 Verifying Connectivity for Oracle Identity Manager

Verify that you can access the administration console, and the Oracle Enterprise Manager Fusion Middleware Control by accessing the URLs mentioned in the table below. The table also provides information about the users who can access these URLS:

Table 7–1 URL and user information for verifying Oracle Identity Manager

URL	User
http://IGDADMIN.mycompany.com:7778/console	weblogic_idm
http://IGDADMIN.mycompany.com:7778/em	weblogic_idm
http://IGDADMIN.mycompany.com:7778/identity	xelsysadm

Table 7–1 (Cont.) URL and user information for verifying Oracle Identity Manager

URL	User
http://IGDADMIN.mycompany.com:7778/sysadmin	xelsysadm
http://IGDADMIN.mycompany.com:7778/apm	oamadmin
http://IGDADMIN.mycompany.com:7778/SchedulerService-web	xelsysadm

Verify that all managed servers are showing a status of Running.

7.1.1.2 Verifying 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 mentioned in the table below. The table also provides information about the users who can access these URLS:

Table 7–2 URL and user information for verifying Oracle Access Management

URL	User
http://IADADMIN.mycompany.com:7777/console	weblogic_idm
http://IADADMIN.mycompany.com:7777/em	weblogic_idm
http://IADADMIN.mycompany.com:7777/oamconsole	oamadmin

Verify that all managed servers are showing a status of Running.

7.1.2 Validating Failover

Test failover of the Access Administration server to OAMHOST2, and then fall back to OAMHOST1 as described in "Manually Failing Over the WebLogic Administration Server" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Test failover of the Identity Governance Administration server to OIMHOST2, and then fall back to OIMHOST1 as described in "Manually Failing Over the WebLogic Administration Server" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

7.2 Validating the Access Manager Configuration

To Validate that this has completed correctly.

1. Access the OAM console at: `http://IADADMIN.mycompany.com/oamconsole`
2. Log in as the `oamadmin` user or the user identified by the entry in Section 4.4.1.10, "Set User Names and Passwords."
3. Click the **System Configuration** tab
4. Click **SSO Agents** in the **Access Manager** section.
5. Click **Search**.
6. You should see the WebGate agents `Webgate_IDM`, `Webgate_IDM_11g`, `IAMSuiteAgent`, and `accessgate-oic`.

7.3 Validating Oracle Identity Manager

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser. at:

`https://SSO.mycompany.com:443/identity`

`https://igdadmin.mycompany.com:443/sysadmin`

Log in using the `xelsysadm` username and password.

7.4 Validating SOA Instance from the WebTier

Validate SOA by accessing the URL:

`http://IDMINTERNAL.mycompany.com:80/soa-infra`

and logging in using the `xelsysadm` username and password.

7.5 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: `http://IADADMIN.mycompany.com/oamconsole`

You now see the Access Manager Login page displayed. Enter your OAM administrator user name (for example, `weblogic`) and password and click **Login**. Then you see the Access Manager console displayed.

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console at `http://IADADMIN.mycompany.com/console` and to Oracle Enterprise Manager Fusion Middleware Control at:
`http://IADADMIN.mycompany.com/em`

The Access Manager Single Sign-On page displays. Provide the credentials for the `weblogic` user to log in.

8

Troubleshooting Oracle Identity and Access Management Deployment

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

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:

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:

8.1.1 Using the Log Files

If you are performing deployment using the wizard, from any phase screen, click 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 the refresh button next to 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. On Linux, this is *LCM_HOME*`/provisioning/logs/`*hostname*.

LCM_HOME is the **Lifecycle Management Store Location** directory that you specified on the Installation and Configuration screen when you created the deployment profile. See Section 4.4.1.8, "Select Installation and Configuration Locations."

8.1.2 Recovering From Oracle Identity and Access Management Deployment Failure

Oracle Identity and Access Management Deployment does not have any backup or recovery mechanism, so you must start from the beginning if case of a failure.

In addition, if you perform a workaround that requires you to rerun Oracle Identity and Access Management Deployment, you must clean up the environment before rerunning it. For more information about cleaning up an environment, see Appendix A, "Cleaning Up an Environment Before Rerunning IAM Deployment".

8.2 Resolving Common Problems

This section describes common problems and solutions. It contains the following topics:

- Section 8.2.1, "Null Error Occurs When WebLogic Patches Are Applied"
- Section 8.2.2, "Identity Management Patch Manager progress Command Shows Active Session After Deployment"
- Section 8.2.3, "Oracle Identity and Access Management Deployment Wizard Hangs (Linux and UNIX)"
- Section 8.2.4, "Error Occurs When Running RCU on 64-bit Linux"
- Section 8.2.5, "Other Identity and Access Management Deployment Issues"

8.2.1 Null Error Occurs When WebLogic Patches Are Applied

Problem

During Oracle Identity and Access Management deployment, patches are applied to all products deployed, including WebLogic. This entails running the Smart Update `bsu` command. This command may fail without producing a detailed error message.

Cause

In this case, the failure is likely caused by directory paths that are longer than what the `bsu` command supports. You can verify this by running the `bsu` command manually, passing it the `-log` option, and looking for a stack trace containing a message such as the following:

```
java.lang.IllegalArgumentException:
Node name
?a?very?long?path?which?may?cause?problems?leading?to?an?IDMTOP?products?dir?utils
?bsu?cache_dir too long
```

For more information, see the chapter "Using the Command Line Interface" in *Oracle Smart Update Applying Patches to OracleWebLogic Server*.

Solution

When planning the IDM deployment, ensure that the `IDM_TOP` path is 45 characters or fewer in length.

8.2.2 Identity Management Patch Manager progress Command Shows Active Session After Deployment

Problem

If you run the Identity Management Patch Manager `progress` command after Oracle Identity and Access Management Deployment completes, the output shows an active session specific to Identity Management Deployment, which is listed as ACTIVE, and contains a set of PLANNED steps.

Solution

You can safely ignore this output. The deployment-driven patch session is complete, and all steps which needed to run have run. Creating a new patch session will silently replace this special session without error.

8.2.3 Oracle Identity and Access Management Deployment Wizard Hangs (Linux and UNIX)

Problem

The Oracle Identity and Access Management Deployment Wizard hangs. Neither the **Next** nor the **Back** button is active.

Cause

This problem is due to stale NFS file handles.

Solution

On Linux or UNIX, issue the following command:

```
df -k
```

Record the output of the df command, even if it is successful, in case further analysis is necessary. For example, take a screenshot.

If the `df` command hangs or is unsuccessful, work with your system administrator fix the NFS problem.

After the NFS problem has been resolved and the `df` command finishes successfully, run deployment again.

8.2.4 Error Occurs When Running RCU on 64-bit Linux

Problem

Repository Creation Utility (RCU) creates the required database schemas for Identity and Access Management components.

On 64-bit Linux, when you try to run RCU by executing the `./rcu` command from the *RCU_HOME*`/bin` directory, the following error message is displayed:

```
Failed to initialize logger with location
:/home/oracle/rcuHome/rcu/log/logdir.2013-02-25_15-42/rcu.log
Initializing logger using the following location :/tmp/logdir.2013-02-25_
15-42/rcu.log
Exception in thread "main" java.lang.UnsatisfiedLinkError:
/home/oracle/rcuHome/jdk/jre/lib/i386/xawt/libmawt.so: libXext.so.6: cannot open
shared object file: No such file or directory
```

```
at java.lang.ClassLoader$NativeLibrary.load(Native Method)
at java.lang.ClassLoader.loadLibrary0(ClassLoader.java:1807)
at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1703)
at java.lang.Runtime.load0(Runtime.java:770)
at java.lang.System.load(System.java:1003)
at java.lang.ClassLoader$NativeLibrary.load(Native Method)
at java.lang.ClassLoader.loadLibrary0(ClassLoader.java:1807)
at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1724)
at java.lang.Runtime.loadLibrary0(Runtime.java:823)
at java.lang.System.loadLibrary(System.java:1028)
at sun.security.action.LoadLibraryAction.run(LoadLibraryAction.java:50)
at java.security.AccessController.doPrivileged(Native Method)
at java.awt.Toolkit.loadLibraries(Toolkit.java:1605)
at java.awt.Toolkit.<clinit>(Toolkit.java:1627)
at com.jgoodies.looks.LookUtils.isLowResolution(LookUtils.java:484)
at com.jgoodies.looks.LookUtils.<clinit>(LookUtils.java:249)
at
com.jgoodies.looks.plastic.PlasticLookAndFeel.<clinit>(PlasticLookAndFeel.java:135
)
at
oracle.sysman.assistants.rcu.ui.InteractiveRCUModel.<init>(InteractiveRCUModel.jav
a:117)
at oracle.sysman.assistants.rcu.Rcu.execute(Rcu.java:307)
at oracle.sysman.assistants.rcu.Rcu.main(Rcu.java:363)
```

Cause

This error message is displayed because RCU is supported only on 32-bit Linux.

Solution

To run RCU on 64-bit Linux, use the following workaround:

1. Go to the *RCU_HOME* directory, and create a backup of the `jdk` directory.

   ```
   cd RCU_HOME
   mv jdk jdk.bak
   ```

2. Create a link to the 64-bit JDK folder using the `ln` command.

   ```
   ln -s /home/oracle/jdk1.6.0_35 jdk
   ```

3. Execute the `./rcu` command from the *RCU_HOME*`/bin` directory.

8.2.5 Other Identity and Access Management Deployment Issues

If you are facing any other deployment issues, see the section "Troubleshooting Identity and Access Management Deployment" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*. This section provides information about some of the other common problems related to deployment.

8.3 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

This appendix describes how to clean up an environment before rerunning Identity and Access Management 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.

To clean up a deployed environment before starting another cycle of deployment, proceed as follows:

1. On each host, stop all Identity and Access Management processes, services and servers using `idmtop/config/scripts/stopall.sh`.
2. Reboot the system to ensure that all server instances are stopped.
3. On each host, remove the contents of the directory *`LOCAL_ROOT`*.

   This is the location on local storage where the OIM managed servers, SOA managed servers, and the OHS instances are stored, for example: `/u02/private/oracle/config`. Note that this directory is available only if you enabled and selected **Local Configuration Location** option on the Select Installation and Configuration Locations screen. For more information, see Section 4.4.1.8, "Select Installation and Configuration Locations".
4. Remove the contents of the directories *`LCM_HOME`* (or *`IDMLCM_HOME`*) and *`IDMTOP`* on shared storage.

   `LCM_HOME` (or *`IDMLCM_HOME`*) 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 4.4.1.8, "Select Installation and Configuration Locations". For information about Oracle and Middle homes, see Section 2.2.3, "Summary of Oracle Homes".

Note: If you are using a Windows system, some Oracle services must be deleted manually. To do this, find the following Oracle services, stop them and then delete each service using the `sc delete` command:

- Oracle VM Service
- Oracle WebLogic NodeManager (C_IDMPROV_BASEDIR_ IDMTOP_products_identity_wlserver_10.3)"
- OracleProcessManager_ohs1
- Oracleagent10gAgent
- Oracleagent10gAgentSNMPPeerEncapsulator
- Oracleagent10gAgentSNMPPeerMasterAgent

Example: `sc delete "Oracle VM Service"`

5. Drop the database schema using RCU. When dropping the schema, ensure that you check the ODS schema because it is not checked by default. IAM deployment will fail during the next run if you do not perform this step correctly.

After you have performed these steps, you can rerun `runIAMDeployment.sh`.