Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E48618-05

September 2014

Documentation for system administrators that describes how to install and configure Oracle Identity and Access Management components in an enterprise deployment for Oracle Fusion Middleware.

ORACLE

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

E48618-05

Primary Authors: Ellen Desmond (Writer), Janga Aliminati (Architect), Michael Rhys (Contributing Engineer)

Contributors: Nagasravani Akula, Christelle Balon, Jeremy Banford, Bruce Jiang, Sindhura Palakodety

Contents

11 Validating Deployment

12 Extending the Domain to Include Oracle Adaptive Access Manager

13 Configuring Server Migration for an Enterprise Deployment

14 Scaling Enterprise Deployments

15 Managing the Topology for an Enterprise Deployment

A Automation of the Process

B Cleaning Up an Environment Before Rerunning IAM Deployment

C Topology Tool Commands for Scaling

List of Figures

List of Tables

Preface

This preface describes the audience, contents and conventions used in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Identity and Access Management enterprise deployments.

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

The following manuals in the Oracle Fusion Middleware documentation library provide additional information on the process of installing and configuring the Enterprise Deployment architecture:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*
- *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 Directory Integration Platform*
- *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 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.

What's New in This Guide

The following topics introduce the new and changed features of Oracle Identity and Access Management and other significant changes that are described in this guide, and provides pointers to additional information.

New and Changed Features for 11*g* Release 2 (11.1.2.2)

Oracle Exalogic Elastic Cloud Enterprise Deployment Guide for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2) differs from previous versions in that the majority of the components are configured using the Identity and Access Management Lifecycle Tools.

This release does not support Oracle Internet Directory or Active Directory as directory stores. Configuring the deployed environment for Oracle Internet Directory or Active Directory must be done outside of the deployment process.

For up-to-date information, see Note: 1662923.1: Updates for Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0). This document is available on My Oracle Support at `https://support.oracle.com`.

1 Enterprise Deployment Overview

This chapter provides an overview of the enterprise topology for Oracle Identity and Access Management.

This chapter contains the following sections:

Oracle Identity and Access Management presents a comprehensive suite of products for all aspects of identity and access management.This guide describes a reference enterprise topology for the Oracle Identity And Access Management Infrastructure components of Oracle Fusion Middleware. It also provides detailed instructions and recommendations to create the topology by following the enterprise deployment guidelines.

1.1 About the Enterprise Deployment Guide

An enterprise deployment is an Oracle best practices blueprint based on proven Oracle high-availability technologies and recommendations for Oracle Fusion Middleware. The high-availability best practices described in this book make up one of several components of high-availability best practices for all Oracle products across the entire technology stack—Oracle Database, Oracle Fusion Middleware, Oracle Applications, and Oracle Enterprise Manager Cloud Control.

An Oracle Fusion Middleware enterprise deployment:

- Considers various business service level agreements (SLA) to make high-availability best practices as widely applicable as possible
- Leverages database grid servers and storage grid with low-cost storage to provide highly resilient, lower cost infrastructure
- Uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs
- Enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster
- Evolves with each Oracle version and is completely independent of hardware and operating system

For more information on high availability practices, see the Oracle Database High Availability page on Oracle Technology Network at:

http://www.oracle.com/technetwork/database/features/availability/index-087701.html

Note: The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* focuses on enterprise deployments in Linux environments. However, you can also implement enterprise deployments using UNIX environments.

1.2 Enterprise Deployment Guide Conventions

All UNIX and Linux command examples shown in this Guide are run using the `bash` shell.

1.3 Enterprise Deployment Terminology

See "Understanding Key Concepts" in *Oracle Fusion Middleware Concepts Guide* for a description of common terms, such as Oracle home and Oracle instance.

This section identifies additional enterprise deployment terminology used in the guide.

- **failover**: When a member of a high availability system fails unexpectedly (unplanned downtime), in order to continue offering services to its consumers, the system undergoes a failover operation. If the system is an active-passive system, the passive member is activated during the failover operation and consumers are directed to it instead of the failed member. The failover process can be performed manually, or it can be automated by setting up hardware cluster services to detect failures and move cluster resources from the failed node to the standby node. If the system is an active-active system, the failover is performed by the load balancer entity serving requests to the active members. If an active member fails, the load balancer detects the failure and automatically redirects requests for the failed member to the surviving active members. See *Oracle Fusion Middleware High Availability Guide* for information on active-active and active-passive systems.
- **failback**: After a system undergoes a successful failover operation, the original failed member can be repaired over time and be re-introduced into the system as a standby member. If desired, a failback process can be initiated to activate this member and deactivate the other. This process reverts the system back to its pre-failure configuration.
- **hardware cluster**: A hardware cluster is a collection of computers that provides a single view of network services (for example: an IP address) or application services (for example: databases, Web servers) to clients of these services. Each node in a hardware cluster is a standalone server that runs its own processes. These processes can communicate with one another to form what looks like a single system that cooperatively provides applications, system resources, and data to users.

  A hardware cluster achieves high availability and scalability through the use of specialized hardware (cluster interconnect, shared storage) and software (health monitors, resource monitors). (The cluster interconnect is a private link used by the hardware cluster for heartbeat information to detect node death.) Due to the need for specialized hardware and software, hardware clusters are commonly provided by hardware vendors such as Sun, HP, IBM, and Dell. While the number

of nodes that can be configured in a hardware cluster is vendor dependent, for the purpose of Oracle Fusion Middleware high availability, only two nodes are required. Hence, this document assumes a two-node hardware cluster for high availability solutions employing a hardware cluster.

- **cluster agent**: The software that runs on a node member of a hardware cluster that coordinates availability and performance operations with other nodes. Clusterware provides resource grouping, monitoring, and the ability to move services. A cluster agent can automate the service failover.
- **clusterware**: A software that manages the operations of the members of a cluster as a system. It allows one to define a set of resources and services to monitor via a heartbeat mechanism between cluster members and to move these resources and services to a different member in the cluster as efficiently and transparently as possible.
- **shared storage**: Shared storage is the storage subsystem that is accessible by all the machines in the enterprise deployment domain. Among other things, the following are located on the shared disk:
  - Middleware Home software
  - AdminServer Domain Home
  - JMS
  - Tlogs (where applicable)

  Managed Server homes can also be optionally located in the shared disk. The shared storage can be a Network Attached Storage (NAS), a Storage Area Network (SAN) or any other storage system that multiple nodes can access simultaneously and can read-write.
- **primary node**: The node that is actively running an Oracle Fusion Middleware instance at any given time and has been configured to have a backup/secondary node. If the primary node fails, Oracle Fusion Middleware instance is failed over to the secondary node. This failover can be manual or automated using the Clusterware for Administration Server. For a server migration based scenario, WebLogic Whole Server Migration is used for automated failover.
- **secondary node**: The node that is the backup node for an Oracle Fusion Middleware instance. This is where the active instance fails over when the primary node is no longer available. See the definition for primary node in this section.
- **network host name**: Network host name is a name assigned to an IP address either through the `/etc/hosts` file or through DNS resolution. This name is visible in the network that the machine to which it refers to is connected. Often, the network host name and physical host name are identical. However, each machine has only one physical host name but may have multiple network host names. Thus, a machine's network host name may not always be its physical host name.
- **physical host name**: This guide differentiates between the terms physical host name and network host name. This guide uses physical host name to refer to the "internal name" of the current machine. On Linux, this is the name returned by the `hostname` command.

  Physical host name is used by Oracle Fusion Middleware to reference the local host. During installation, the installer automatically retrieves the physical host name from the current machine and stores it in the Oracle Fusion Middleware configuration metadata on disk.

- **physical IP**: Physical IP refers to the IP of a machine on the network. In almost all cases, it is normally associated with the physical host name of the machine (see the definition of the physical host name). In contrast to a virtual IP, it is always associated with the same machine when on a network.
- **switchover**: During normal operation, active members of a system may require maintenance or upgrading. A switchover process can be initiated to allow a substitute member to take over the workload performed by the member that requires maintenance or upgrading, which undergoes planned downtime. The switchover operation ensures continued service to consumers of the system.
- **switchback**: When a switchover operation is performed, a member of the system is deactivated for maintenance or upgrading. When the maintenance or upgrading is completed, the system can undergo a switchback operation to activate the upgraded member and bring the system back to the pre-switchover configuration.
- **virtual host name**: Virtual host name is a network addressable host name that maps to one or more physical machines via a load balancer or a hardware cluster. For load balancers, the name "virtual server name" is used interchangeably with virtual host name in this book. A load balancer can hold a virtual host name on behalf of a set of servers, and clients communicate indirectly with the machines using the virtual host name. A virtual host name in a hardware cluster is a network host name assigned to a cluster virtual IP. Because the cluster virtual IP is not permanently attached to any particular node of a cluster, the virtual host name is not permanently attached to any particular node either.

  Note: Whenever the term "virtual host name" is used in this document, it is assumed to be associated with a virtual IP address. In cases where just the IP address is needed or used, it will be explicitly stated.

- **virtual IP**: Also, cluster virtual IP and load balancer virtual IP. Generally, a virtual IP can be assigned to a hardware cluster or load balancer. To present a single system view of a cluster to network clients, a virtual IP serves as an entry point IP address to the group of servers which are members of the cluster. A virtual IP can be assigned to a server load balancer or a hardware cluster.

  A hardware cluster uses a cluster virtual IP to present to the outside world the entry point into the cluster (it can also be set up on a standalone machine). The hardware cluster's software manages the movement of this IP address between the two physical nodes of the cluster while clients connect to this IP address without the need to know which physical node this IP address is currently active on. In a typical two-node hardware cluster configuration, each machine has its own physical IP address and physical host name, while there could be several cluster IP addresses. These cluster IP addresses float or migrate between the two nodes. The node with current ownership of a cluster IP address is active for that address.

  A load balancer also uses a virtual IP as the entry point to a set of servers. These servers tend to be active at the same time. This virtual IP address is not assigned to any individual server but to the load balancer which acts as a proxy between servers and their clients.

These will be described in more detail in the following chapters.

1.4 Benefits of Oracle Recommendations

The Oracle Fusion Middleware configurations discussed in this guide are designed to ensure security of all transactions, maximize hardware resources, and provide a reliable, standards-compliant system for enterprise computing with a variety of applications. The security and high availability benefits of the Oracle Fusion Middleware configurations are realized through isolation in firewall zones and replication of software components.

This section contains the following topics:

1.4.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own zone, and all traffic is restricted by protocol and port. The following characteristics ensure security at all needed levels, as well as a high level of standards compliance:

- All external communication received on port 80 (*HTTP_PORT*) is redirected to port 443 (*HTTP_SSL_PORT*).
- External communication uses the Secure Socket Layer (SSL) secure Web Protocol. This is terminated at the site's load balancer.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the data tier zone is allowed.
- Components are separated between zones on the web tier, application tier, and database tier.
- Direct communication across two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- LDAP directories can be isolated in a directory tier zone. (Oracle Unified Directory is in the application tier zone).
- Identity And Access Management components are in the application tier zone.
- All communication between components across zones is restricted by port and protocol, according to firewall rules.

1.4.2 High Availability

The Enterprise Deployment architectures are highly available because each component or functional group of software components is replicated on a different computer and configured for component-level high availability.

2

Introduction and Planning

This chapter describes and illustrates the enterprise deployment reference topology employed in this guide.

The key to a successful Enterprise 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 topics:

2.1 Planning Your Deployment

An enterprise deployment for Identity And Access Management consists of the following parts:

- A highly available database for storing policy information and information specific to the identity and access management components being deployed.
- Identity And Access Management components installed in a highly available manner to support the creation and management of identity information, as well as to restrict access to resources based on the policies and identities stored within the database and identity store. 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, to restrict access to those components and to ascertain the identity of people and processes trying to gain access to corporate resources.
- A highly available load balancer, which is used to distribute load between the web servers. The load balancer can also be 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.

There are many ways that these component parts can be put together. This guide explains in detail how to deploy one topology. This topology is not the only one supported by Oracle, but it is deemed to be the most common.

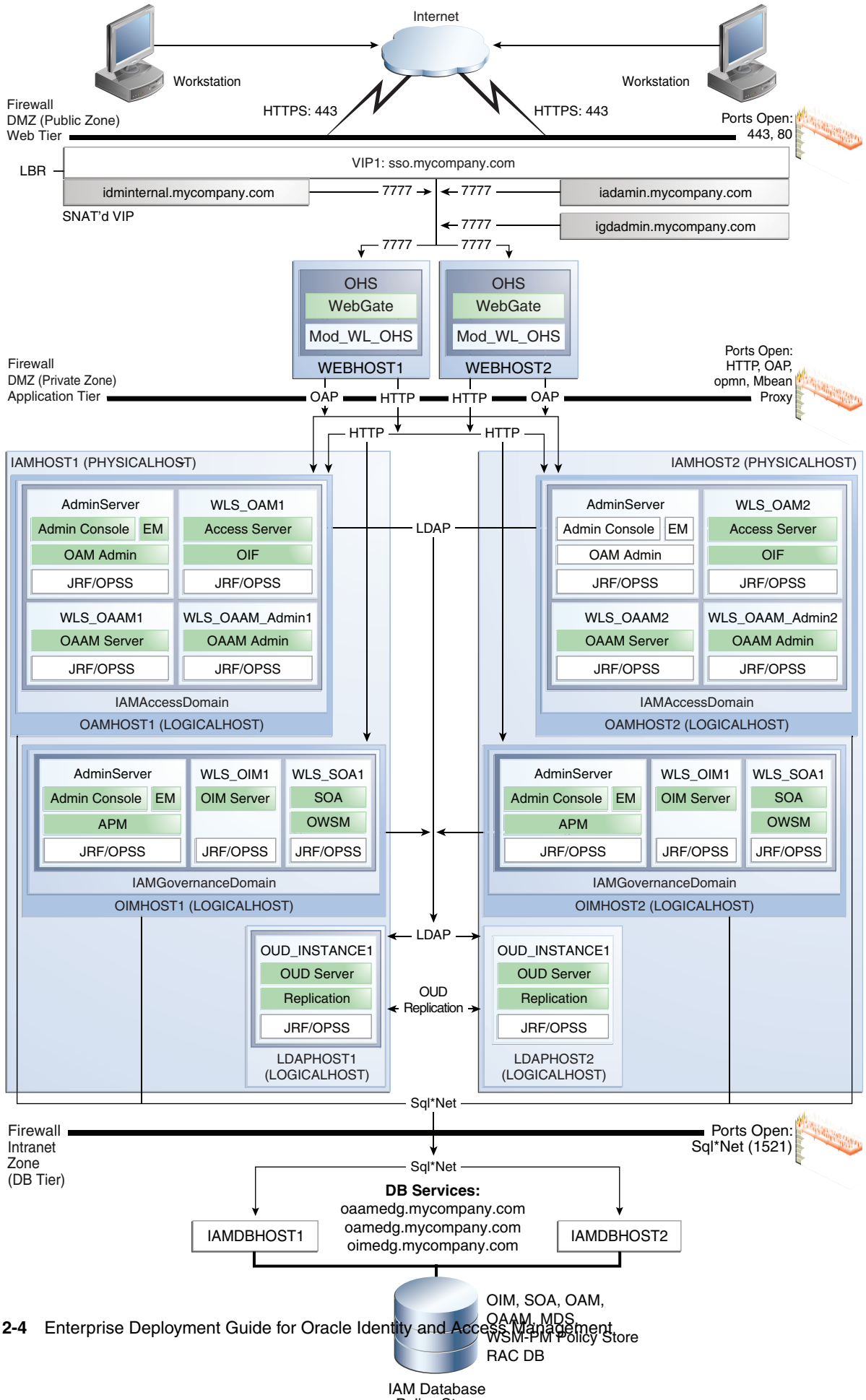
This section contains the following topics:

2.1.1 Deployment Topology

A topology is a deployment map of components. There are several different ways that Oracle Identity and Access Management components can be installed to provide a working Identity and Access management solution. A topology can also be described as an architectural blueprint. This guide shows a common deployment topology for Oracle Identity and Access Management.

There are many different ways that Oracle Identity and Access Management can be deployed in an Enterprise Deployment. The two most common deployment models involve placing everything into a single domain and separating operational and managerial components into different domains. The figure below shows the split domain deployment model.

Figure 2–1 Split Domain Topology


Internet
Workstation
Workstation
Firewall
DMZ (Public Zone)
Web Tier
HTTPS: 443
HTTPS: 443
Ports Open:
443, 80
LBR
VIP1: sso.mycompany.com
idminternal.mycompany.com
SNAT'd VIP
7777
7777
iadamin.mycompany.com
7777
igdadmin.mycompany.com
7777
7777
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS
WebGate
Mod_WL_OHS
WEBHOST2
Firewall
DMZ (Private Zone)
Application Tier
OAP
HTTP
HTTP
OAP
Ports Open:
HTTP, OAP,
opmn, Mbean
Proxy
HTTP
HTTP
IAMHOST1 (PHYSICALHOST)
IAMHOST2 (PHYSICALHOST)
AdminServer
Admin Console
EM
OAM Admin
JRF/OPSS
WLS_OAM1
Access Server
OIF
JRF/OPSS
WLS_OAAM1
OAAM Server
JRF/OPSS
WLS_OAAM_Admin1
OAAM Admin
JRF/OPSS
IAMAccessDomain
OAMHOST1 (LOGICALHOST)
LDAP
AdminServer
Admin Console
EM
OAM Admin
JRF/OPSS
WLS_OAM2
Access Server
OIF
JRF/OPSS
WLS_OAAM2
OAAM Server
JRF/OPSS
WLS_OAAM_Admin2
OAAM Admin
JRF/OPSS
IAMAccessDomain
OAMHOST2 (LOGICALHOST)
AdminServer
Admin Console
EM
APM
JRF/OPSS
WLS_OIM1
OIM Server
JRF/OPSS
WLS_SOA1
SOA
OWSM
JRF/OPSS
IAMGovernanceDomain
OIMHOST1 (LOGICALHOST)
AdminServer
Admin Console
EM
APM
JRF/OPSS
WLS_OIM1
OIM Server
JRF/OPSS
WLS_SOA1
SOA
OWSM
JRF/OPSS
IAMGovernanceDomain
OIMHOST2 (LOGICALHOST)
LDAP
OUD_INSTANCE1
OUD Server
Replication
JRF/OPSS
LDAPHOST1
(LOGICALHOST)
OUD
Replication
OUD_INSTANCE1
OUD Server
Replication
JRF/OPSS
LDAPHOST2
(LOGICALHOST)
Sql*Net
Firewall
Intranet
Zone
(DB Tier)
Ports Open:
Sql*Net (1521)
Sql*Net
DB Services:
oaamedg.mycompany.com
oamedg.mycompany.com
oimedg.mycompany.com
IAMDBHOST1
IAMDBHOST2
OIM, SOA, OAM,
OAAM, MDS,
WSM-PM Policy Store
RAC DB
IAM Database

This figure is a graphical representation of the enterprise topology. It 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. The instructions in this guide describe how to install and configure the software for this topology.

For more information, refer to Section 2.3, "Understanding the Topology."

The topology is divided into tiers, including the following:

2.1.1.1 The Web Tier

There are two servers, each of which hosts an Oracle HTTP Server and Oracle WebGate.

2.1.1.2 The Application Tier

The Application Tier consists of the following components:

- An Oracle WebLogic Administration Server for each domain. Inside the administration server are managerial and navigational components for the domain, such as: Oracle WebLogic Console, Oracle Enterprise Manager Fusion Middleware Control, and Access Management Console.

  A 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. The WebLogic managed servers for Oracle Access Management are placed into a domain called IAMAccessDomain, and the managed servers for Oracle Identity Manager and SOA components are placed into a domain called IAMGovernanceDomain
- Oracle Access Management Access Manager, which hosts Access Server, Federation and corresponding Java Required Files/Oracle Platform Security Services processes
- Oracle Adaptive Access Manager Server and Oracle Adaptive Access Management Administration and corresponding Java Required Files/Oracle Platform Security Services processes
- Oracle Identity Manager, which hosts an Oracle Identity Manager Server and corresponding JRF/OPSS processes
- Oracle SOA, which hosts a SOA Server and corresponding Java Required Files/Oracle Platform Security Services processes
- Oracle Unified Directory, which is the LDAP directory for identity information. Oracle Unified Directory instance is kept up to date through Oracle Unified Directory replication.

The Application Tier components in the figure are shown on logical hosts within physical hosts. These logical hosts can be virtual machines or lower specification hardware servers.You can deploy these components either in a distributed topology, using the logical hosts, or in a consolidated topology where the logical hosts are combined into larger physical hosts.

Distributed Topology

In a Distributed Topology the Application Tier components are located as follows:

Table 2–1 Location of Components in a Distributed Topology

Machine	Component	Domain
OAMHOST1	WebLogic Administration Server	IAMAccessDomain
	Oracle Access Management Access Manager	
	Oracle Adaptive Access Manager	
OIMHOST1	WebLogic Administration Server	IAMGovernanceDomain
	Oracle Identity Manager	
	Oracle SOA	
	Oracle Authorization Policy Manager	
LDAPHOST1	Oracle Unified Directory	
OAMHOST2	WebLogic Administration Server (Passive)	IAMAccessDomain
	Oracle Access Management Access Manager	
	Oracle Adaptive Access Manager	
OIMHOST2	WebLogic Administration Server (Passive)	IAMGovernanceDomain
	Oracle Identity Manager	
	Oracle SOA	
LDAPHOST2	Oracle Unified Directory	

Consolidated Topology

In a Consolidated Topology the Application Tier components are located as follows:

Table 2–2 Location of Components in a Consolidated Topology

Machine	Component	Domain
IAMHOST1	WebLogic Administration Server	IAMAccessDomain
	Oracle Access Management Access Manager	
	Oracle Adaptive Access Manager	
	WebLogic Administration Server	IAMGovernanceDomain
	Oracle Identity Manager	
	Oracle SOA	
	Oracle Authorization Policy Manager	
	Oracle Unified Directory	

Table 2–2 (Cont.) Location of Components in a Consolidated Topology

Machine	Component	Domain
IAMHOST2	WebLogic Administration Server (Passive)	IAMAccessDomain
	Oracle Access Management Access Manager	
	Oracle Adaptive Access Manager	
	WebLogic Administration Server (Passive)	IAMGovernanceDomain
	Oracle Identity Manager	
	Oracle SOA	
	Oracle Unified Directory	

Oracle Adaptive Access Manager is an optional component in the deployment.

2.1.1.3 The Data Tier

This is where the databases reside. The databases contain customer data and the schemas required by the application tier products.

2.1.1.4 The Load Balancer

Inside the demilitarized zone (DMZ) is a load balancer which directs requests received on SSO.mycompany.com, IADADMIN.mycompany.com and IDMINTERNAL.mycompany.com and directs requests to the Oracle HTTP servers. In the case of SSO.mycompany.com, requests are SSL encrypted. This is terminated at the load balancer. IGDADMIN.mycompany.com and IDMINTERNAL.mycompany.com handle requests using the HTTP protocol.

In addition, the load balancer distributes LDAP requests among the Oracle Unified Directory instances on LDAPHOST1 and LDAPHOST2, using the load balancer virtual host IDSTORE.mycompany.com

2.1.1.5 Firewalls

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

2.1.2 Benefits of Using the Split Domain Topology

The split domain topology is suitable for large organizations requiring individual control over each component in the deployment.

The main advantages of the Split Domain topology are related to patching flexibility. Specifically:

- As each component (Oracle Identity Manager and Access Manager) reside in different domains, you can apply patches (even domain level ones) so that they update only the component they are targeted at.
- You can patch Administrative Components such as Oracle Identity Manager without the need for a controlled outage, which you would require when updating an Operational component such as Access Manager).

2.2 About Oracle Directory Services Manager

Oracle Directory Services Manager provides direct access to the configuration and data installed inside the LDAP directory. This is considered a development tool and is therefore not included in the Enterprise Deployment topology.

2.3 Understanding the Topology

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 within that tier.

This section contains the following topics:

- Section 2.3.1, "About the Web Tier"
- Section 2.3.2, "About the Application Tier"
- Section 2.3.3, "About the Optional Directory Tier"
- Section 2.3.4, "About the Database Tier,"

2.3.1 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 for most enterprise deployments, the web tier is desirable. To support enterprise level single sign-on using products such as Oracle Single Sign-On and Access Manager, the web tier is required.

While components such as Oracle Enterprise Manager Fusion Middleware Control and WebLogic Console can function without a web tier, they can be configured to use a web tier, if desired.

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.
- WebGate (an Oracle Access Management Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with 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. Port 443 is open.

2.3.1.1 Architecture Notes

Oracle HTTP Servers on WEBHOST1 and WEBHOST2 are configured with mod_wl_ohs, to proxy requests to Oracle Identity and Access Management J2EE applications deployed in WebLogic Servers on OAMHOST1, OAMHOST2, OIMHOST1, and OIMHOST2.

2.3.1.2 High Availability Provisions

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

2.3.1.3 Security Provisions

The Oracle HTTP Servers process requests received using the URLs `SSO.mycompany.com`, `IGDADMIN.mycompany.com`, and `IADADMIN.mycompany.com`. The names `IADADMIN.mycompany.com` and `IGDADMIN.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.

2.3.2 About the Application Tier

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

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. However, for the enterprise deployment shown in Figure 1-1, customers have a separate web tier relying on web servers such as Apache or Oracle HTTP Server.

The application tier includes the following components. Their locations within the application tier are described in Table 2–1, " Location of Components in a Distributed Topology" and Table 2–2, " Location of Components in a Consolidated Topology".

- Oracle Access Management Access Manager (OAM). This is an J2EE applications which is run within Oracle WebLogic Server.
- Oracle Adaptive Access Manager (OAAM).
- Oracle Identity Manager and Oracle Entitlements Server Policy Manager, which are used for user provisioning and policy management.
- The governance components, which are Oracle Authorization Policy Manager (APM), 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. Note: These servers also run Oracle SOA which is used exclusively by Oracle Identity Manager. Oracle Identity Manager (OIM) communicates with the directory tier.

In addition:

- OAMHOST1 in the distributed topology, or IAMHOST1 in the consolidated topology, 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 Management console.
- OIMHOST1 in the distributed topology, or IAMHOST1 in the consolidated topology, 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.

2.3.2.1 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. Conversely, you can use a single domain to centralize all WebLogic Server administration activities.

In the topology used in this version of the guide, Access and Governance domains are in separate WebLogic Server domains from the one where customer applications might be deployed. Oracle Identity Manager is deployed into a separate, dedicated domain so that it can be patched independently of other products.

2.3.2.2 About LDAP Directories

Identity information is stored with an LDAP compliant directory. In this implementation, it is Oracle Unified Directory. Oracle Unified Directory is an all-in-one directory solution with storage, proxy, synchronization and virtualization capabilities. It ensures scalability to billions of entries, ease of installation, elastic deployments, enterprise manageability and effective monitoring. Its flexible deployment architecture provides high performance levels to meet application requirements.

Note: This release of *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* does not support Oracle Internet Directory and Active Directory as directory stores. Configuring the deployed environment for Oracle Internet Directory or Active Directory must be done outside of the Deployment process

---

The standard LDAP port is 389 *(LDAP_LBR_PORT)* for the non-SSL port and 636 (*LDAP_LBR_SSL_PORT*) for the SSL port. LDAP services are often used for white

pages lookup by clients such as email clients in the intranet. The ports 389 and 636 on the load balancer are typically redirected to the non-privileged ports used by the individual directory instances. LDAP requests are distributed among the Oracle Unified Directory hosts using a hardware load balancer.

Many organizations have an existing directory deployment. If you do not have an existing deployment, then you can use this guide to learn how to configure Oracle Unified Directory to take on this role. If you have an existing directory, you can use this guide to learn how to configure that directory for use with Oracle Identity and Access Management. If you do not have a directory and you want to use a directory other than Oracle Unified Directory, refer to your directory documentation for information about configuring these directories in a highly available manner.

Oracle Unified Directory stores information locally in a Berkeley database. To ensure high availability, this information is replicated to other Oracle Unified Directory instances using Oracle Unified Directory replication.

Oracle Unified Directory server instances natively use replication to keep their embedded databases in sync. By default, replication employs a loose consistency model in which the updates are replicated to replicas AFTER returning the operation result to the application. In this model it is therefore possible to write some data to a replica, and read outdated information from another replica for a short time after the write. Great efforts have been made in Oracle Unified Directory replication to ensure that the replication process is fast and can achieve replication in the order of one millisecond.

Oracle Unified Directory can be configured to use the Assured Replication model, which has been developed to guarantee that the data in the replicas is consistent. When using the Safe Read mode of Assured Replication, applications have the guarantee that the replication process is completed before returning the result of a write operation.

Using Assured Replication has a negative impact on the response time of write operations because it requires some communications with remote replicas before returning the operation result. The amount of the delay varies, depending on the network being used and the capacity of the servers hosting Oracle Unified Directory. Using Assured replication has little if any impact on read operations.

If you expect to regularly perform large writes to your directory, consider configuring your load balancer to distribute requests to your Oracle Unified Directory instances in an active/passive mode. This will remove the chance of you reading out of date data from a replica, but could result in overall performance degradation if your Oracle Unified Directory host is not capable of processing all of the requests.

For the purposes of this Guide, it is assumed that the ability to have multiple servers processing requests is more important than the extra overhead incurred with writing requests in Assured mode. To that end, this Guide shows the configuration of Oracle Unified Directory using Assured Replication. Both of the following Oracle Unified Directory configurations, however, are supported:

- Active/Active in an assured configuration
- Active/Passive in a non assured configuration

For more information, see the Assured Replication section of *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

Oracle Unified Directory normally keeps track of changes by using an internal change number. The change number is specific to each Oracle Unified Directory instance, which can cause issues if one Oracle Unified Directory instance fails without the entry being replicated. Such a failure can impact Oracle Identity Manager reconciliation.

Note: There is no automatic restart if Oracle Unified Directory fails. Oracle Unified Directory relies on requests being redirected to a surviving instance by the load balancer.

2.3.2.3 Architecture Notes

- An embedded version of Oracle Entitlement Server is used to control access to Oracle Fusion Middleware components.
- Oracle Entitlements Server uses a centralized policy store that is stored within a database.
- Oracle Adaptive Access Manager is an optional component.
- Access Manager uses the OPSS Policy Store to store policy information.
- In a split domain configuration, Oracle Identity Manager and SOA are installed into a separate domain from other components.
- The Oracle WebLogic Server console, Oracle Enterprise Manager Fusion Middleware Control, and Access Management console are always bound to the listen address of an Administration Server.
- The WebLogic administration server is a singleton service. It runs on only one node at a time. In the event of failure, it is restarted on a surviving node.
- The managed servers WLS_OAM1 and WLS_OAM2 are deployed in a cluster and Access Manager applications deployed to the cluster.
- The managed servers WLS_OIM1 and WLS_OIM2 are deployed in a cluster and Identity Manager applications deployed to the cluster.
- The managed servers WLS_SOA1 and WLS_SOA2 are deployed in a cluster and Identity Manager applications deployed to the cluster.

2.3.2.4 High Availability Provisions

- Access Manager Server, Oracle Identity Manager, and SOA are active-active deployments; these servers communicate with the data tier at run time.
- The WebLogic Administration Server and Oracle Enterprise Manager deployment is active-passive (where other components are active-active). There is one Administration Server per domain.
- The WebLogic Administration Server is a singleton component deployed in an active-passive configuration. If the primary fails or an Administration Server does not start on its assigned host, the Administration Server can be started on a secondary host. If a WebLogic managed server fails, the node manager running on that host attempts to restart it.

2.3.2.5 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.

2.3.3 About the Optional Directory Tier

No directory tier is shown in Section 2.1.1, "Deployment Topology," as this Guide features the use of Oracle Unified Directory, which typically resides in the application tier. You can also put Oracle Unified Directory in a directory tier for added security, as

the directory tier is typically protected by firewalls. Applications above the directory tier access LDAP services through a designated LDAP host port and sometimes a management port, which should be opened in that firewall.

The directory tier is typically managed by directory administrators providing enterprise LDAP service support.

2.3.4 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 data 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.

Although not shown in the diagram, you might be required to place directories into the Database tier for added security.

2.4 Hardware Requirements for an Enterprise 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.

These servers should have the minimum specification shown in Table 2–3, " Typical Hardware Requirements for a Distributed Topology" or Table 2–4, " Typical Hardware Requirements for a Consolidated Topology".

For detailed requirements, or for requirements for other platforms, see *Oracle Fusion Middleware System Requirements and Specifications*.

Table 2–3 Typical Hardware Requirements for a Distributed Topology

Server	Processor	Disk	Memory	TMP Directory	Swap
Database Host IAMDBHOST*n*	4 or more X Pentium 1.5 GHz or greater	nXm n=Number of disks, at least 4 (striped as one disk). m=Size of the disk (minimum of 30 GB)	6-16 GB	Default	Default
WEBHOST*n*	2 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default
OIMHOST*n*	6 or more X Pentium 1.5 GHz or greater	10 GB	8 GB	Default	Default
OAMHOST*n*	6 or more X Pentium 1.5 GHz or greater	10 GB	8 GB	Default	Default
LDAPHOST*n*	2 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default

Table 2–4 Typical Hardware Requirements for a Consolidated Topology

Server	Processor	Disk	Memory	TMP Directory	Swap
Database Host IAMDBHOST*n*	4 or more X Pentium 1.5 GHz or greater	nXm n=Number of disks, at least 4 (striped as one disk). m=Size of the disk (minimum of 30 GB)	6-16 GB	Default	Default
WEBHOST*n*	2 or more X Pentium 1.5 GHz or greater	25 GB	4 GB	Default	Default
IAMHOST*n*	6 or more X Pentium 1.5 GHz or greater	30 GB	25 GB	Default	Default

These are the typical hardware requirements. For each tier, carefully consider the load, throughput, response time and other requirements to plan the actual capacity required. The number of nodes, CPUs, and memory required can vary for each tier based on the deployment profile.Production requirements may vary depending on applications and the number of users.

The Enterprise Deployment configurations described in this guide use two servers for each tier to provide failover capability. This, however, does not presume adequate computing resources for any application or user population. If the system workload increases such that performance is degraded, you can add WebLogic servers or directory/OHS instances as described in Section 14.4, "Scaling the Web Tier."

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

2.5 Software Components for an Enterprise Deployment

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

This section contains the following topics:

- Section 2.5.1, "Software Versions"
- Section 2.5.2, "About Obtaining Software"
- Section 2.5.3, "Summary of Oracle Homes"
- Section 2.5.4, "Applying Patches and Workarounds"

2.5.1 Software Versions

Table 2–5, " Software Versions Used" lists the Oracle software you need to obtain before starting the procedures in this guide.

Table 2–5 Software Versions Used

Short Name	Product	Version
OHS11G	Oracle HTTP Server	11.1.1.7.0

Table 2–5 (Cont.) Software Versions Used

Short Name	Product	Version
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 Assistant	11.1.2.2.0
OUD	Oracle Unified Directory	11.1.2.2.0

2.5.2 About Obtaining Software

To perform an automated installation of Oracle Identity and Access Management 11g Release 2 (11.1.2.2), download the Oracle Identity and Access Management Deployment Repository 11.1.2.2.0 from:

- The Oracle Software Delivery Cloud: http://edelivery.oracle.com/
- The Oracle Identity and Access Management download page: http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/oid-11gr2-2104316.html

Note:

- If you downloaded a version of the Oracle Identity and Access Management Deployment Repository prior to April 8, 2014, you must replace it with a newer version before proceeding.
- If you are running RCU on a 64-bit Linux machine which does not have 32-bit system libraries available, you must either install such libraries for compatibility, or separately download the 64-bit version of RCU 11.1.2.2.0 and use that instead of the one present in the Deployment Repository.

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

2.5.3 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 2–6 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 2–6 Summary of Homes

Home Name	Home Description	Products Installed
IAD_MW_HOME	The Oracle Middleware Home containing the *ORACLE_HOME*s required by Oracle Identity Manager.	
IGD_MW_HOME	The Oracle Middleware Home containing the *ORACLE_HOME*s required by Oracle Access Manager.	
DIR_MW_HOME	The Oracle Middleware Home containing the *ORACLE_HOME*s required by Oracle Unified Directory.	
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*.	Oracle WebLogic Server
IAD_ORACLE_HOME	Contains the binary and library files required for Oracle Identity and Access Management and is located in *IAD_MW_HOME*/iam.	Access Manager
IGD_ORACLE_HOME	Contains the binary and library files required for Oracle Identity and Access Management and is located in *IGD_MW_HOME*/iam.	Oracle Identity Manager
OUD_ORACLE_HOME	Contains the binary and library files required for Oracle Unified Directory and is located in *IAD_MW_HOME*/oud	Oracle Unified Directory
WEBGATE_ORACLE_HOME	Contains the binaries for Oracle WebGate and is located in *WEB_MW_HOME*/web.	Oracle WebGate
SOA_ORACLE_HOME	Contains the binary and library files required for the Oracle SOA Suite. Located in *IGD_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
LCM_HOME	Lifecycle Repository.	
REPOS_HOME	Software Repository.	
WEB_MW_HOME	The Oracle Middleware Home containing the ORACLE_HOMEs required by the web tier.	
WEB_ORACLE_HOME	Contains the binary and library files required for Oracle HTTP server.	

2.5.4 Applying Patches and Workarounds

See the Oracle Fusion Middleware Release Notes for your platform and operating system for a list of patches to apply. You **must** apply the patches to ensure that your software operates as expected.

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

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.

Download the patches from http://support.oracle.com and unzip each patch to the directory appropriate for the product, as listed in Table 2–7. If the directory does not exist, create it.

After unzipping the patch make sure that the Patch Directory (as listed in Table 2–7) contains a directory which is a number. That directory contains directories and files similar to:

- etc
- files
- README.txt

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

bundle_patch_no/*product*/*product_patch_no*

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

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

Table 2–7 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

2.6 Road Map for the Reference Topology Installation and Configuration

Before beginning your Oracle Identity and Access Management enterprise deployment, review the flow chart in Figure 2–2, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process". This flow chart illustrates the high-level process for completing the enterprise deployment documented in this guide. Table 2–8 describes the steps in the flow chart and directs you to the appropriate section or chapter for each step.

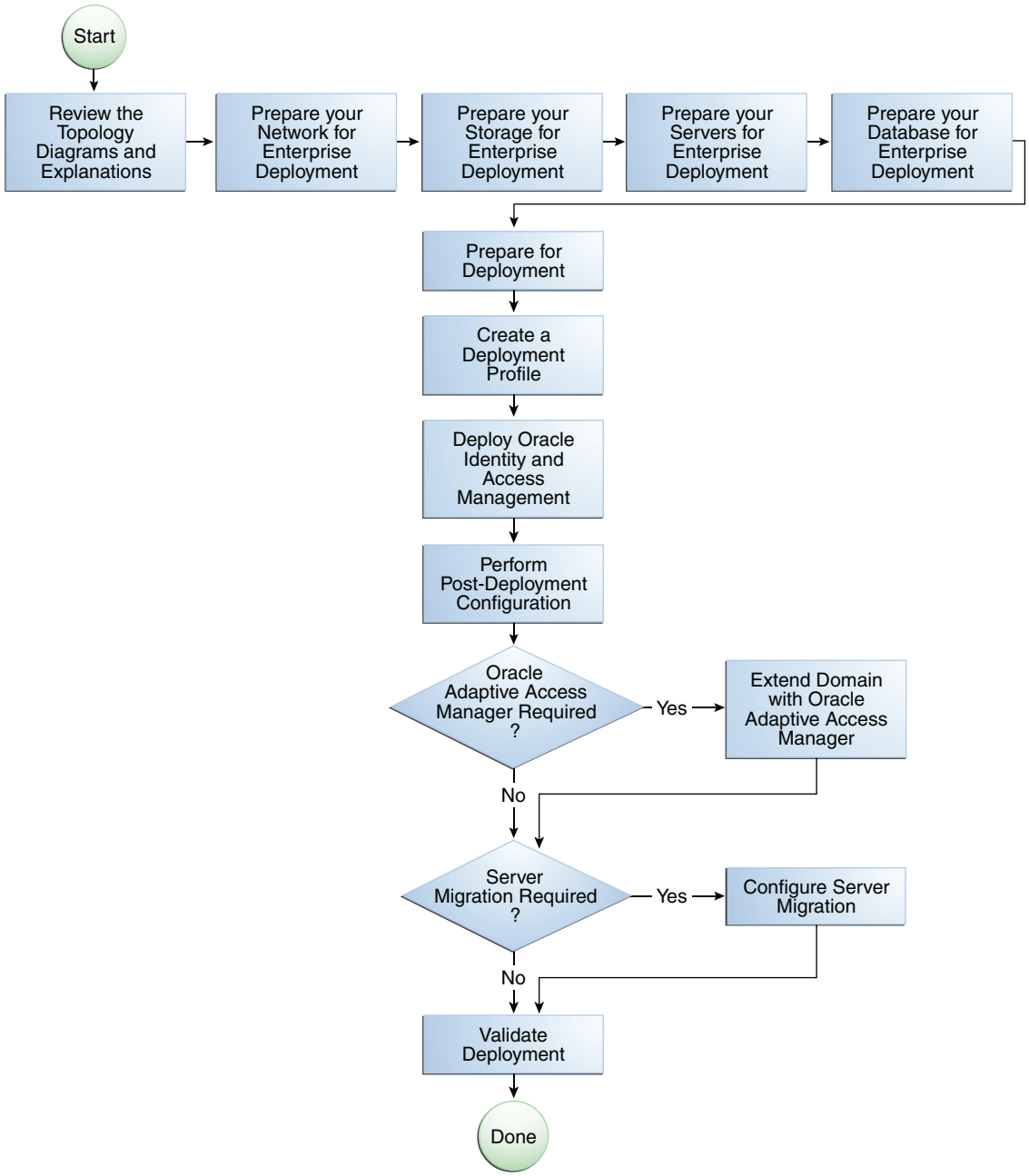
This section covers the following topics:

- Section 2.6.1, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process"
- Section 2.6.2, "Steps in the Oracle Identity and Access Management Enterprise Deployment Process"

2.6.1 Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process

Figure 2–2, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process" provides a flow chart of the Oracle Identity and Access Management enterprise deployment process. Review this chart to become familiar with the steps that you must follow, based on the existing environment.

Figure 2–2 Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process



2.6.2 Steps in the Oracle Identity and Access Management Enterprise Deployment Process

Table 2–8 describes each of the steps in the enterprise deployment process flow chart for Oracle Identity and Access Management, shown in Figure 2–2. The table also provides information on where to obtain more information about each step in the process.

Table 2–8 Steps in the Oracle Identity and Access Management Enterprise Deployment Process

Step	Description	More Information
Prepare your Network for Enterprise Deployment	To prepare your network for an enterprise deployment, understand concepts, such as virtual server names and IPs and virtual IPs, and configure your load balancer by defining virtual host names.	Chapter 3, "Preparing the Network for an Enterprise Deployment"
Prepare your Storage for Enterprise Deployment	To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared and local storage.	Chapter 4, "Preparing Storage for an Enterprise Deployment"
Prepare your Servers for an Enterprise Deployment	To prepare your servers for an enterprise deployment, ensure that your servers meet hardware and software requirements, enable Unicode support and Virtual IP Addresses, mount shared storage, configure users and groups, and, if necessary, install software onto multihomed systems.	Chapter 5, "Configuring the Servers for an Enterprise Deployment"
Prepare automation (optional)	Prepare scripts for One command deployment if desired	Appendix A, "Automation of the Process"
Prepare your Database for Enterprise Deployment	To prepare your database for an enterprise deployment, review database requirements, create database services, load the metadata repository in the Oracle RAC database, configure Identity and Access Management schemas for transactional recovery privileges, and back up the database.	Chapter 6, "Preparing the Database for an Enterprise Deployment"
Prepare for Deployment	To prepare for Deployment, assemble required information, create a repository, verify Java, install the tools, and verify port availability	Chapter 7, "Preparing for Deployment"
Create a Deployment Profile	Run the wizard to create a Deployment response file.	Chapter 8, "Creating a Deployment Profile"
Deploy Identity and Access Management	Use the tools to perform all stages of Deployment.	Chapter 9, "Deploying Identity and Access Management"

Table 2–8 (Cont.) Steps in the Oracle Identity and Access Management Enterprise Deployment Process

Step	Description	More Information
Perform Post-Deployment Configuration	Perform post-Deployment tasks.	Chapter 10, "Performing Post-Deployment Configuration"
Validate Deployment	Perform validation checks.	Chapter 11, "Validating Deployment"
Extend a Domain to Include Oracle Adaptive Access Manager	Extend the domain with this optional component.	Chapter 12, "Extending the Domain to Include Oracle Adaptive Access Manager"

2.7 Additional Documentation

For up-to-date information, see Note: 1662923.1: Updates for Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0). This document is available on My Oracle Support at `https://support.oracle.com`.

3

Preparing the Network for an Enterprise Deployment

This chapter describes the prerequisites for the Oracle Identity and Access Management Infrastructure enterprise deployment topology.

This chapter includes the following topics:

3.1 Overview of Preparing the Network for an Enterprise Deployment

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.

3.2 Planning Your Network

As shown in the deployment topology figures in Section 2.3, "Understanding the Topology," each deployment can be spread across multiple zones. A zone is a means of restricting access to components of your infrastructure to those that actually need it. In the examples in this guide, two zones are shown.

- The public zone–This is where the outside world gains access to your systems. You place into this zone only those components that the outside world must access, such as the Load Balancers and Web Tiers. If users from the outside world attempts to access any servers or services below this zone, they are prevented from doing so by firewalls.

  The public zone is configured so that the servers in this zone can interact with the application servers in the private zone.

- The intranet zone–This is where you place servers that contain core services, such as databases. These services are very tightly controlled by the organization as they contain the most sensitive data.

By using this approach, you restrict access to information to only those components that require it. This approach is useful where you have users coming in from outside of your organization.

If, instead of an extranet, you are setting up an intranet, where all communication is from trusted sources, then you might reasonably decide to do away with one or more of the zones.

3.3 Virtual Server Names Used by the Topology

Virtual Server names are used to hide the identities of the real host names used by the organization, and are used as the entry points into the applications.

One benefit of using virtual server names is that the backend server names can change without the application having to be reconfigured with new host names.

Another advantage of using virtual server names is that these server names can be attached to a load balancer, allowing the load balancer to use a single name to distribute requests amongst a number of back end servers which serve the same function. This ensures availability and simplified scalability.

When attached to a load balancer the load balancer can also terminate SSL allowing the applications to maintain encrypted traffic between the application and the client but at the same time to allow the application to perform more efficiently without having to encrypt traffic between each component.

Virtual Server names are included in the organizations DNS servers. External application entries are configured in external DNS servers.

This ensures that public access points are resolvable in the internet and private access points available only inside the organization.

On Prem Only:

Some of the virtual servers, such as IDSTORE.mycompany.com and IDMINTERNAL, you may wish to exclude from DNS altogether and to resolve only those servers you are using.

Both:

Virtual Server Names resolve to a single IP address. This IP address can be associated with a virtual host on a load balancer.

Exalogic:

- IDSTORE.mycompany.com
- IADADMIN.mycompany.com
- IGDADMIN.mycompany.com
- IDMINTERNAL.mycompany.com
- SSO.mycompany.com

Ensure that the virtual server names are associated with IP addresses and are part of your DNS. The computers on which Oracle Fusion Middleware is running must be able to resolve these virtual server names.

You define the virtual server names on the load balancer using the procedure in Section 3.4, "Configuring the Hardware Load Balancers"

The rest of this guide assumes that the deployment is one of those shown in Chapter 2, "Introduction and Planning."

3.3.1 IDSTORE.mycompany.com

- This virtual server acts as the access point for all Identity Store LDAP traffic. Traffic to both the SSL and non-SSL is configured. The clients access this service using the address `IDSTORE.mycompany.com:636` for SSL and `IDSTORE.mycompany.com:389` for non-SSL.
- Because your Identity Store in Oracle Unified Directory is accessed directly, you must monitor the heartbeat of the Oracle Unified Directory processes. If an Oracle Unified Directory process stops, the load balancer must continue to route the LDAP traffic to a surviving Oracle Unified Directory instance.
- This virtual server directs traffic received on port 389 *(LDAP_LBR_PORT)* to each of the Oracle Unified Directory instances on port 1389 (*LDAP_DIR_PORT*).
- This virtual server directs traffic received on port 1636 (*LDAP_LBR_SSL_PORT*) to each of the Oracle Unified Directory instances on port 1636 *(LDAP_DIR_SSL_PORT*).
- This virtual server is resolvable only locally (in Exalogic).

3.3.2 IADADMIN.mycompany.com

- This virtual server acts as the access point for all internal HTTP traffic that gets directed to the administration services in the Access Domain. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `IADADMIN.mycompany.com:80` and in turn forward these to port 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2. The services accessed on this virtual host include the WebLogic Administration Server Console and Oracle Enterprise Manager Fusion Middleware Control.
- This virtual server is resolvable in the corporate DNS only.
- Create rules in the firewall to block outside traffic from accessing the `/console`, `/oamconsole`, `/oaam_admin`, and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IADADMINVHN.mycompany.com` virtual host.

3.3.3 IGDADMIN.mycompany.com

- This virtual server acts as the access point for all internal HTTP traffic that gets directed to the administration services in the Governance Domain. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `IGDADMIN.mycompany.com:80` (*HTTP_PORT*) and in turn forward these to ports 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2. The services accessed on this virtual host include the WebLogic Administration Server Console, and Oracle Enterprise Manager Fusion Middleware Control,and Oracle Authorization Policy Manager.
- Create rules in the firewall to block outside traffic from accessing the `/sysadmin`, `/apm`, `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IGDADMINVHN.mycompany.com` virtual host.

- This virtual server should be resolvable only in the corporate DNS.

3.3.4 IDMINTERNAL.mycompany.com

- The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `IDMINTERNAL.mycompany.com:80` and in turn forward these to port `7777` (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2. The SOA Managed servers access this virtual host to callback Oracle Identity Manager web services
- Create rules in the firewall to block outside traffic from accessing this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IDMINTERNAL.mycompany.com` virtual host.
- This virtual server should be resolvable either locally or in the corporate DNS
- Because `IDMINTERNAL` is designed for interprocess communication, you might want to NOT include this in DNS, but have it resolvable only in internal host files.

3.3.5 SSO.mycompany.com

- This is the virtual name which fronts all Identity and Access Management components, including Access Manager and Oracle Identity Manager.
- This virtual server acts as the access point for all HTTP traffic that gets directed to the single sign on services. The incoming traffic from clients is SSL enabled. Thus, the clients access this service using the address `SSO.mycompany.com:443` and in turn forward these to port 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2. All the single sign on enabled protected resources are accessed on this virtual host.
- Configure this virtual server in the load balancer with both port 80 (*HTTP_PORT*) and port 443 (*HTTP_SSL_PORT)*.
- This virtual server should be resolvable either locally or in the corporate DNS
- This virtual host must be configured to preserve the client IP address for a request. In some load balancers, you configure this by enabling the load balancer to insert the original client IP address of a request in an X-Forwarded-For HTTP header.

3.4 Configuring the Hardware Load Balancers

A hardware load balancer directs requests to the application in this case Oracle Identity and Access Management to the individual hosts which make up the application components.

A load balancer is configured with virtual hosts. Each virtual host is associated with a different IP address, which is serviced by the load balancer. The Load balancer virtual host is then associated with a pool of origin servers consisting of the web servers in the deployment.

Virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring. These should be configured to route request to the appropriate real hosts and ports running the services. 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.

There are two load balancer devices in the recommended topology. One load balancer is set up for external HTTP traffic and the other load balancer is set up for internal LDAP traffic. A deployment may choose to have a single load balancer device due to a variety of reasons. While this is supported, the deployment should consider the security implications of doing this and if found appropriate, open up the relevant firewall ports to allow traffic across the various zones. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant mode.

This section contains the following topics:

3.4.1 Load Balancer Requirements

The enterprise topology uses an external load balancer. This external load balancer must have the following features:

- Ability to load-balance traffic to a pool of real servers through a virtual server name: Clients access services using the virtual server name (instead of using actual server names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration.
- Monitoring of ports (HTTP and HTTPS).
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
  - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle WebLogic Clusters, the load balancer must be configured with a virtual server and ports for HTTP and HTTPS traffic.
  - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- Resource monitoring / port monitoring / process failure detection: The load balancer must be able to detect service and node failures (through notification or some other means) and to stop directing non-Oracle Net traffic to the failed node. If your external load balancer has the ability to automatically detect failures, you should use it.
- Fault tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- Sticky routing capability: Ability to maintain sticky connections to components based on cookies or URL.

- Other: It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- SSL acceleration, which refers to off loading the public-key encryption algorithms involved in SSL transactions to a hardware accelerator. This feature is recommended, but not required.
- Ability to terminate SSL requests at the load balancer and forward traffic to the backend real servers using the equivalent non-SSL protocol. For example, the load balancer must be able to forward HTTPS requests as HTTP. This feature is sometimes called "SSL termination." It is required for this Enterprise Deployment.
- Ability to Preserve the Client IP Addresses: The Load Balancer must have the capability to insert the original client IP address of a request in an X-Forwarded-For HTTP header to preserve the Client IP Address.
- Ability to add `WL-Proxy-SSL: true` to the HTTP Request Header. Some load balancers do this automatically.

3.4.2 Load Balancer Configuration Procedures

The procedures for configuring a load balancer differ, depending on the specific type of load balancer. Refer to the vendor supplied documentation for actual steps. The following steps outline the general configuration flow:

1. Create a pool of servers. This pool contains a list of servers and the ports that are included in the load balancing definition. For example, for load balancing between the web hosts you create a pool of servers which would direct requests to the web servers in the topology which accept requests using port 7777 (*`WEB_HTTP_PORT`*).
2. Create rules to determine whether or not a given host and service is available and assign it to the pool of servers described in Step 1.
3. Create a Virtual Server on the load balancer. This is the address and port that receives requests used by the application. For example, to load balance Web Tier requests you would create a virtual server for `SSO.mycompany.com:80`.
4. If your load balancer supports it, specify whether or not the virtual server is available internally, externally or both. Ensure that internal addresses are only resolvable from inside the network.
5. Configure SSL Termination, if applicable, for the virtual server.
6. Assign the Pool of servers created in Step 1 to the virtual server.
7. Tune the time out settings as listed in Table 3–3, " Ports Used in the Oracle Identity and Access Management Enterprise Deployment Topology". This includes time to detect whether a service is down.

3.4.3 Load Balancer Configuration

For an Identity and Access Management deployment, configure your load balancer as shown in Table 3–1.

Table 3–1 Load Balancer Configuration

Virtual Host	Server Pool	Protocol	SSL Termination	External	Other Required Configuration/Comments
SSO.mycompany.com:80 (*HTTP_PORT*)	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	Yes	Identity and Access Management requires that the following be added to the HTTP header: Header Name: IS_SSL Header Value: ssl
SSO.mycompany.com:443 (*HTTP_SSL_PORT*)	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTPS	Yes	Yes	Identity and Access Management requires that the following be added to the HTTP header: Header Name: IS_SSL Header Value: ssl
IADADMIN.mycompany.com:80 (*HTTP_PORT*)	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	No	IADADMINVHN.mycompany.com:80 (*HTTP_PORT*)
IGDADMIN.mycompany.com:80 (*HTTP_PORT*)	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	No	IGDADMINVHN.mycompany.com:80 (*HTTP_PORT*)
IDMINTERNAL.mycompany.com:80 (*HTTP_PORT*)	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	No	
IDSTORE.mycompany.com:389	LDAPHOST1.mycompany.com:1389 LDAPHOST2.mycompany.com:1389	LDAP	No	No	Only required if Identity and Access Management users are stored in an Oracle Unified Directory.

Table 3–1 (Cont.) Load Balancer Configuration

Virtual Host	Server Pool	Protocol	SSL Termination	External	Other Required Configuration/Comments
IDSTORE.mycompany.com:636	LDAPHOST1.mycompany.com:1636 LDAPHOST2.mycompany.com:1636	LDAPS	No	No	Only required if Identity and Access Management users are stored in an Oracle Unified Directory.

3.5 About IP Addresses and Virtual IP Addresses

A virtual IP address is an unused IP Address which belongs to the same subnet as the host's primary IP address. It is assigned to a host manually and Oracle WebLogic Managed servers are configured to listen on this IP Address. In the event of the failure, the IP address is assigned to another node in the same subnet, so that the new node can take responsibility for running the managed servers assigned to it.

The following is a list of the Virtual IP addresses required by Oracle Identity and Access Management:

- IADADMINVHN.mycompany.com

  In Enterprise deployments the WebLogic Administration Server must be able to continue processing requests after the host it is residing on fails. A virtual IP address should be provisioned in the application tier so that it can be bound to a network interface on any host in the application tier. The WebLogic Administration Server is configured later to listen on this virtual IP address, as discussed later in this manual. The virtual IP address fails over along with the Administration Server from OAMHOST1 to OAMHOST2, or vice versa.

- IGDADMINVHN.mycompany.com

  In Enterprise deployments the WebLogic Administration Server must be able to continue processing requests after the host it is residing on fails. A virtual IP address should be provisioned in the application tier so that it can be bound to a network interface on any host in the application tier. The WebLogic Administration Server is configured later to listen on this virtual IP address, as discussed later in this manual. This virtual IP address fails over along with the Administration Server from OIMHOST1 to OIMHOST2, or vice versa.

- SOAHOSTxVHN.mycompany.com

  One virtual IP address is required for each SOA managed server. This enables the servers to participate in Server migration.

  Provision a virtual IP address in the application tier so that it can be bound to a network interface on any host in the application tier.

- OIMHOSTxVHN.mycompany.com

  One virtual IP Address is required for each Oracle Identity Manager managed server. This enables the servers to participate in Server migration.

  Provision a virtual IP address in the application tier so that it can be bound to a network interface on any host in the application tier.

Configure the Administration Server and the managed servers to listen on different virtual IPs and physical IPs as illustrated in Figure 3–1.

Figure 3–1 IP Addresses and VIP Addresses–Distributed

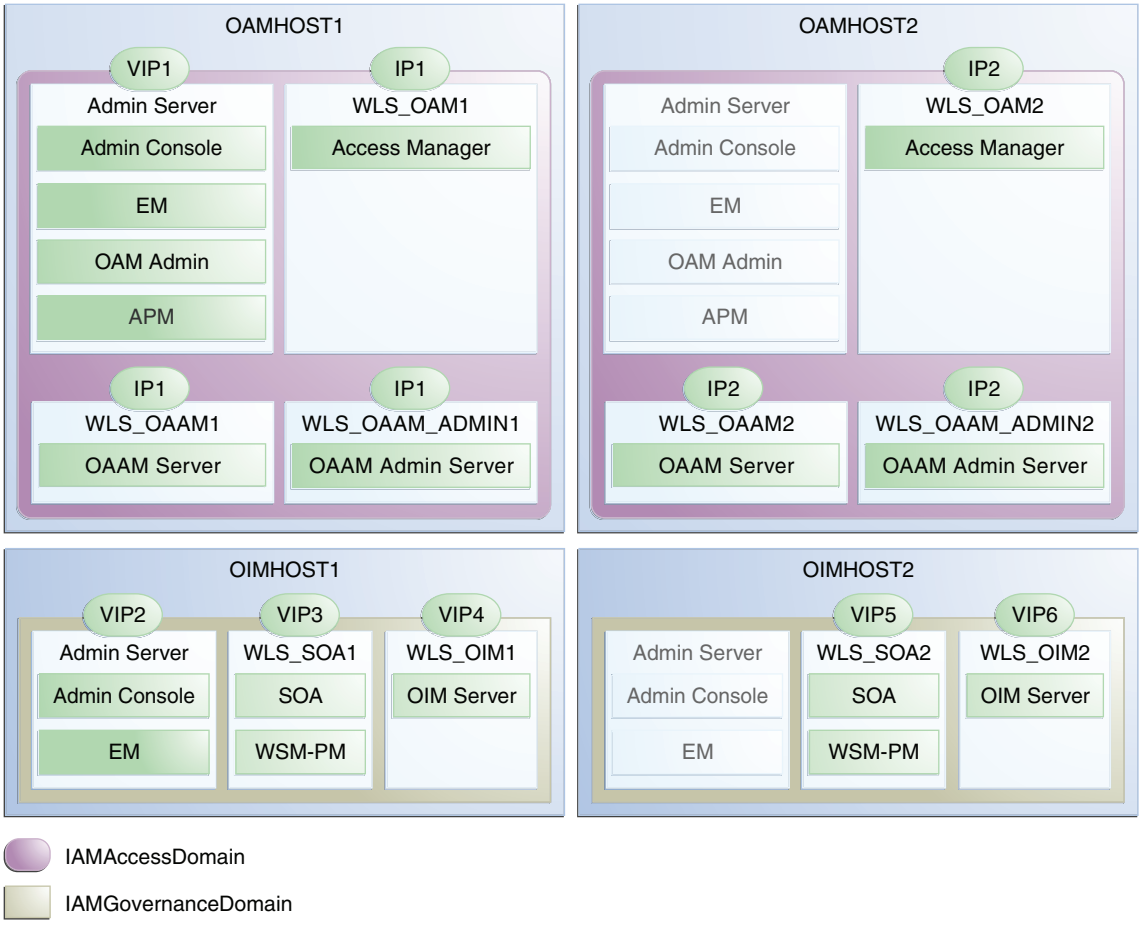


Figure 3–2 IP Addresses and VIP Addresses–Consolidated

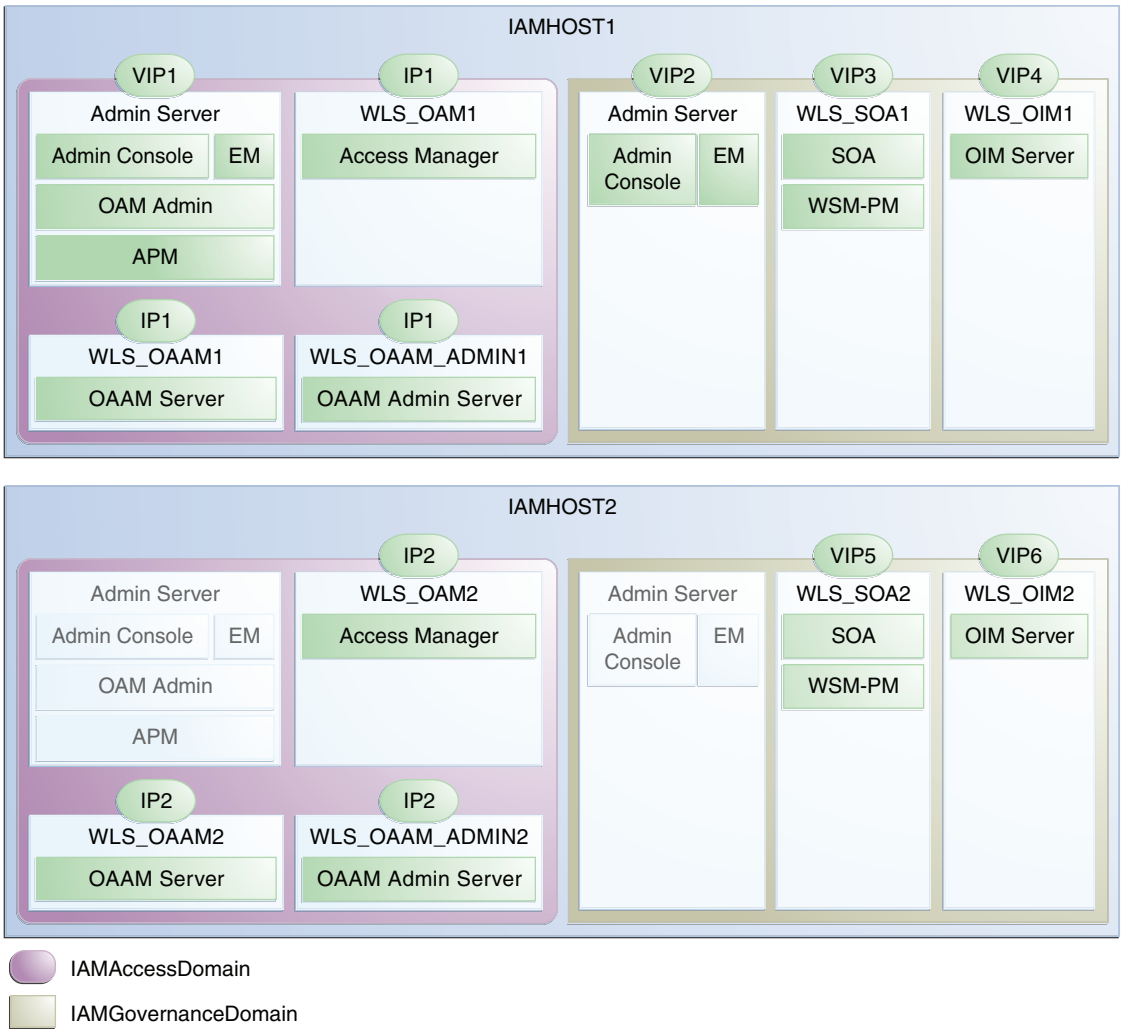


Table 3–2 provides descriptions of the various virtual hosts.

Table 3–2 VIP Addresses and Virtual Hosts

Virtual IP	VIP Maps to...	Description (Consolidated)	Default Host (Consolidated)	Default Host (Distributed)
VIP1	IADADMINVHN	IADADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running.	IAMHOST1	OAMHOST1
VIP2	IGDADMINVHN	IGDADMINVHN is the virtual host name that is the listen address for the Oracle Identity Manager Administration Server. It fails over with manual failover of the Administration Server. It is enabled on the node where the Oracle Identity Manager Administration Server process is running.	IAMHOST1	OIMHOST1

Table 3–2 (Cont.) VIP Addresses and Virtual Hosts

Virtual IP	VIP Maps to...	Description (Consolidated)	Default Host (Consolidated)	Default Host (Distributed)
VIP3	SOAHOST1VHN	SOAHOST1VHN is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA1 process is running.	IAMHOST1	OIMHOST1
VIP4	OIMHOST1VHN	OIMHOST1VHN is the virtual host name that maps to the listen address for the WLS_OIM1 server and fails over with server migration of this server. It is enabled in the node where the WLS_ OIM1 process us running.	IAMHOST1	OIMHOST1
VIP5	SOAHOST2VHN	SOAHOST2VHN is the virtual host name that maps to the listen address for WLS_SOA2 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA2 process is running.	IAMHOST2	OIMHOST2
VIP6	OIMHOST2VHN	OIMHOST2VHN is the virtual host name that maps to the listen address for the WLS_OIM2 server and fails over with server migration of this server. It is enabled in the node where the WLS_ OIM2 process us running.	IAMHOST2	OIMHOST2

3.6 Configuring Firewalls and Ports

Many Oracle Fusion Middleware components and services use ports. As an administrator, you must know the port numbers used by these services, and to ensure that the same port number is not used by two services on a host.

Most port numbers are assigned after installation. You can use different port numbers if you want to. The port numbers shown in Table 3–3 are examples that are used throughout this guide for consistency. If you use different port numbers, you must substitute those values for the values in the table wherever they are used.

Table 3–3 lists the ports used in the Oracle Identity and Access Management topology, including the ports that you must open on the firewalls in the topology.

Firewall notation:

- FW0 refers to the outermost firewall.
- FW1 refers to the firewall between the web tier and the application tier.
- FW2 refers to the firewall between the application tier and the database tier.

Table 3–3 Ports Used in the Oracle Identity and Access Management Enterprise Deployment Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Browser request	FW0	80	HTTP / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity and Access Management.
Browser request	FW0	443	HTTPS / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity and Access Management.
Browser request	FW1	80	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IAM.
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IAM.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 3.4, "Configuring the Hardware Load Balancers."
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
Webtier Access to Oracle Weblogic Administration Server (IAMAccessDomain)	FW1	7001	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Webtier Access to Oracle Weblogic Administration Server (IAMGovernanceDomain)	FW1	7101	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Enterprise Manager Agent - web tier to Enterprise Manager	FW1	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
Oracle HTTP Server to WLS_OAM	FW1	14100	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the `mod_weblogic` parameters used.
Oracle HTTP Server WLS_OIM	FW1	14000	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the mod_ weblogic parameters used
Oracle HTTP Server WLS_SOA	FW1	8001	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the mod_ weblogic parameters used
Oracle HTTP Server management by Administration Server	FW1	OPMN remote port (6701) and OHS Administration Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period, such as 5-10 seconds.
Access Manager Server	FW1	5575	OAP	Both	N/A
Access Manager Coherence port	FW1	9095	TCMP	Both	N/A

Table 3–3 (Cont.) Ports Used in the Oracle Identity and Access Management Enterprise Deployment

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
OAAM Server port	FW1	14300	HTTP / Enterprise Manager	Both	N/A
OAAM Administration port	FW1	14200	HTTP / Enterprise Manager	Both	N/A
Oracle Coherence Port	FW1	8000 - 8088	TCMP	Both	N/A
WLS_OAAM to Administration Server	FW2	OPMN remote port	HTTP / Administration Server to OPMN	Inbound	N/A
Application Tier to Database Listener	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Identity and Access Management.
Oracle Notification Server (ONS)	FW2	6200	ONS	Both	Required for Gridlink. An ONS server runs on each database server.
OUD Port	FW2	1389	LDAP	Inbound	Ideally, these connections should be configured not to time out.
OUD SSL Port	FW2	14636	LDAPS	Inbound	Ideally, these connections should be configured not to time out.
Load Balancer LDAP Port	FW2	386	LDAP	Inbound	Ideally, these connections should be configured not to time out.
Load Balancer LDAP SSL Port	FW2	636	LDAPS	Inbound	Ideally, these connections should be configured not to time out.
Node Manager	N/A	5556	TCP/IP	N/A	N/A
Oracle Unified Directory Replication	N/A	8989	TCP/IP	N/A	N/A

Note: Additional ports might need to be opened across the firewalls to enable applications in external domains, such as SOA or WebCenter Portal domains, to authenticate against this Identity and Access Management domain.

3.7 Managing Access Manager Communication Protocol

This section discusses Oracle Access Protocol (OAP) and provides an overview of a user request.

This section contains the following topics:

- Section 3.7.1, "Access Manager Protocols"
- Section 3.7.2, "Overview of Integration Requests"
- Section 3.7.3, "Overview of User Request"
- Section 3.7.4, "About the Multicast Requirement for Communication"
- Section 3.7.5, "Verifying Network Connectivity"

3.7.1 Access Manager Protocols

Oracle Access Protocol (OAP) enables communication between Access System components (for example, Access Manager Server, WebGate) during user authentication and authorization. This protocol was formerly known as NetPoint Access Protocol (NAP) or COREid Access Protocol.

3.7.2 Overview of Integration Requests

Oracle Access Management Access Manager is responsible for creating sessions for users. When Access Manager is integrated with another Identity and Access Management component, such as Oracle Identity Manager, authentication is delegated to that component.

A typical request flow is as follows:

1. The user tries to access a resource for the first time.
2. WebGate intercepts the request and detects that the user is not authenticated.
3. Access Manager credential collector is invoked and the user enters a user name and password in response to a prompt. Access Manager knows that password policy requires the password to be changed at first login, so the user's browser is redirected to Oracle Identity Manager.
4. The user is prompted to change password and set up challenge questions.
5. At this point, Oracle Identity Manager has authenticated the user using the newly entered password. Oracle Identity Manager creates a TAP request to say that Access Manager can create a session for the user. That is, the user will not be expected to log in again. This is achieved by adding a token to the user's browser that Access Manager can read.

   The TAP request to Access Manager will include such things as:

   - Where the Access Manager servers are located.
   - What web gate profile to use.
   - WebGate profile password.
   - Certificates, if Access Manager is working in simple or cert mode.

3.7.3 Overview of User Request

The request flow when a user requests access is as follows:

1. The user requests access to a protected resource over HTTP or HTTPS.
2. The WebGate intercepts the request.
3. The WebGate forwards the request to the Access Manager Server over Oracle Access Protocol to determine if the resource is protected, how, and whether the user is authenticated (if not, there is a challenge).
4. The Access Manager Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate over Oracle Access Protocol, and generates an encrypted cookie to authenticate the user.
5. Following authentication, the WebGate prompts the Access Manager Server over Oracle Access Protocol and the Access Manager Server looks up the appropriate security policies, compares them to the user's identity, and determines the user's level of authorization.

- If the access policy is valid, the user is allowed to access the desired content and/or applications.
- If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

3.7.4 About the Multicast Requirement for Communication

Oracle recommends that the nodes in the topology communicate using unicast communication. Unlike multicast communication, unicast does not require cross-network configuration. Using unicast avoids network errors due to multicast address conflicts.

In unicast messaging mode, the default listening port of the server is used if no channel is configured. Cluster members communicate to the group leader when they need to send a broadcast message which is usually the heartbeat message. When the cluster members detect the failure of a group leader, the next oldest member becomes the group leader. The frequency of communication in unicast mode is similar to the frequency of sending messages on multicast port.

The following considerations apply when using unicast to handle cluster communications:

- All members of a WebLogic cluster must use the same message type. Mixing multicast and unicast messaging is not allowed.
- Individual cluster members cannot override the cluster messaging type.
- The entire cluster must be shut down and restarted to change the message modes from unicast to multicast or from multicast to unicast.
- JMS topics configured for multicasting can access WebLogic clusters configured for unicast because a JMS topic publishes messages on its own multicast address that is independent of the cluster address. However, the following considerations apply:
  - The router hardware configurations that allow unicast clusters may not allow JMS multicast subscribers to work.
  - JMS multicast subscribers need to be in a network hardware configuration that allows multicast accessibility. (That is, JMS subscribers must be in a multicast-enabled network to access multicast topics.

Note: Although you can set up cluster communication using Unicast, Oracle Identity Manager depends upon Multicast when it is used for caching. For that reason, you must enable multicast between the machines.

3.7.5 Verifying Network Connectivity

After having defined the Network, ensure that all of the network names are resolvable from each of the compute Nodes/vServers.

You do this by performing the following command on each compute node/vServer

```
ping -I interface hostname
```

4

Preparing Storage for an Enterprise Deployment

This chapter describes how to prepare storage for an Oracle Identity and Access Management enterprise deployment.

The storage model described in this guide was chosen for maximum availability, best isolation of components, symmetry in the configuration, and facilitation of backup and disaster recovery. The rest of the guide uses a directory structure and directory terminology based on this storage model. Other directory layouts are possible and supported.

This chapter contains the following topics:

4.1 Overview of Preparing Storage for Enterprise Deployment

It is important to set up your storage in a way that makes the enterprise deployment easier to understand, configure, and manage. Oracle recommends setting up your storage according to information in this chapter. The terminology defined in this chapter is used in diagrams and procedures throughout the guide.

Use this chapter 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 this guide is chosen for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

4.2 Terminology for Directories and Directory Variables

This section describes the directory variables used throughout this guide for configuring the Oracle Identity and Access Management enterprise deployment. You are not required to set these as environment variables. The following directory variables are used to describe the directories installed and configured in the guide:

- **ORACLE_BASE**: This environment variable and related directory path refers to the base directory under which Oracle products are installed.

- **MW_HOME**: This variable and related directory path refers to the location where Oracle Fusion Middleware resides. A *MW_HOME* has a *WL_HOME*, an *ORACLE_COMMON_HOME* and one or more *ORACLE_HOMEs*.

  There is a different *MW_HOME* for each product suite.

  In this guide, this value might be preceded by a product suite abbreviation, for example: *DIR_MW_HOME*, *IAD_MW_HOME*, *IGD_MW_HOME*, and *WEB_MW_HOME*.

- **WL_HOME**: This variable and related directory path contains installed files necessary to host a WebLogic Server. The WL_HOME directory is a peer of Oracle home directory and resides within the *MW_HOME*.

- **ORACLE_HOME**: This variable points to the location where an Oracle Fusion Middleware product, such as Oracle HTTP Server or Oracle SOA Suite is installed and the binaries of that product are being used in a current procedure. In this guide, this value might be preceded by a product suite abbreviation, for example: IAD_ORACLE_HOME, IGD_ORACLE_HOME, WEB_ORACLE_HOME, WEBGATE_ORACLE_HOME, SOA_ORACLE_HOME, and OUD_ORACLE_HOME.

  For more information about homes, see Table 2–6, " Summary of Homes".

- **ORACLE_COMMON_HOME**: This variable and related directory path refer to the location where the Oracle Fusion Middleware Common Java Required Files (JRF) Libraries and Oracle Fusion Middleware Enterprise Manager Libraries are installed. An example is: *MW_HOME*/oracle_common

- **ORACLE_INSTANCE**: An Oracle instance contains one or more system components, such as Oracle Web Cache or Oracle HTTP Server. An Oracle instance directory contains updatable files, such as configuration files, log files, and temporary files.

  In this guide, this value might be preceded by a product suite abbreviation, such as WEB_ORACLE_INSTANCE.

- **JAVA_HOME**: This is the location where Oracle JRockit is installed.

- **ASERVER_HOME**: This path refers to the file system location where the Oracle WebLogic domain information (configuration artifacts) are stored.

  There is a different ASERVER_HOME for each domain used, specifically: IGD_ASERVER_HOME and IAD_ASERVER_HOME

- **MSERVER_HOME**: This path refers to the local file system location where the Oracle WebLogic domain information (configuration artifacts) are stored.This directory is generated by the pack/unpack utilities and is a subset of the ASERVER_HOME. It is used to start and stop managed servers. The Administration Server is still started from the ASERVER_HOME directory.

  There is a different MSERVER_HOME for each domain used. Optionally, it can be used to start and stop managed servers.

- **LCM_HOME**: This is the location of the life cycle management tools and software repository.

For more information about, and examples of these variables, see Section 4.4.4, "Recommended Directory Locations."

4.3 About File Systems

After you create the partitions on your storage, you must place file systems on the partitions so that you can store the Oracle files. For local or direct attached shared

storage, the file system type is most likely the default type for your operating system, for example: EXT3 for Linux.

If your shared storage is on network attached storage (NAS), which is accessed by two or more hosts either exclusively or concurrently, then you must use a supported clustered file system such as NFS version 3 or 4. Such file systems provide conflict resolution and locking capabilities.

4.4 About Recommended Locations for the Different Directories

This section contains the following topics:

- Section 4.4.1, "Recommendations for Binary (Middleware Home) Directories"
- Section 4.4.2, "Recommendations for Domain Configuration Files"
- Section 4.4.3, "Shared Storage Recommendations for JMS File Stores and Transaction Logs"
- Section 4.4.4, "Recommended Directory Locations"

4.4.1 Recommendations for Binary (Middleware Home) Directories

The following sections describe guidelines for using shared storage for your Oracle Fusion Middleware middleware home directories:

- Section 4.4.1.1, "About the Binary (Middleware Home) Directories"
- Section 4.4.1.2, "About Sharing a Single Middleware Home"
- Section 4.4.1.3, "About Using Redundant Binary (Middleware Home) Directories"

4.4.1.1 About the Binary (Middleware Home) Directories

When you install any Oracle Fusion Middleware product, you install the product binaries into a Middleware home. The binary files installed in the Middleware home are read-only and remain unchanged unless the Middleware home is patched or upgraded to a newer version.

In a typical production environment, the Middleware home files are saved in a separate location from the domain configuration files, which you create using the Oracle Fusion Middleware Configuration Wizard.

The Middleware home for an Oracle Fusion Middleware installation contains the binaries for Oracle WebLogic Server, the Oracle Fusion Middleware infrastructure files, and any Oracle Fusion Middleware product-specific directories.

If you have your LDAPHOSTs in a different zone from your application hosts, it may be desirable not to share the Binary installation location across zones. If you are adopting this model and want to have a separate location for LDAP binaries, create two shares for the binaries on your SAN: one for the Application Tier binaries and one for the directory binaries. The first share will be mounted on the application tier servers and the second share mounted on the directory tier servers. While the shares are different they will be mounted on the servers using the same mount point. For example: `/u01/oracle/products`

The Web tier binaries are not shared. These are placed onto local storage so that SAN storage does not have to be mounted in the DMZ.

For more information about the structure and content of an Oracle Fusion Middleware home, see *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite*.

4.4.1.2 About Sharing a Single Middleware Home

Oracle Fusion Middleware enables you to configure multiple Oracle WebLogic Server domains from a single Middleware home. This allows you to install the Middleware home in a single location on a shared volume and reuse the Middleware home for multiple host installations.

When a Middleware home is shared by multiple servers on different hosts, there are some best practices to keep in mind. In particular, be sure that the Oracle Inventory on each host is updated for consistency and for the application of patches.

To update the oraInventory for a host and attach a Middleware home on shared storage, use the following command:

```
ORACLE_HOME/oui/bin/attachHome.sh
```

For more information about the Oracle inventory, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer Concepts Guide.*

4.4.1.3 About Using Redundant Binary (Middleware Home) Directories

For maximum availability, Oracle recommends using redundant binary installations on shared storage.

In this model, you install two identical Middleware homes for your Oracle Fusion Middleware software on two different shared volumes. You then mount one of the Middleware homes to one set of servers, and the other Middleware home to the remaining servers. Each Middleware home has the same mount point, so the Middleware home always has the same path, regardless of which Middleware home the server is using.

Should one Middleware home become corrupted or unavailable, only half your servers are affected. For additional protection, Oracle recommends that you disk mirror these volumes.

If separate volumes are not available on shared storage, Oracle recommends simulating separate volumes using different directories within the same volume and mounting these to the same mount location on the host side. Although this does not guarantee the protection that multiple volumes provide, it does allow protection from user deletions and individual file corruption.

This is normally achieved post deployment by performing the following steps:

1. Create a new shared volume for binaries.
2. Leave the original mounted volume on odd numbered servers. for example: OAMHOST1, OIMHOST1
3. Mount the new volume in the same location on even mounted servers, for example: OAMHOST2, OIMHOST2
4. Copy the files on volume1 to volume2 by copying from an odd numbered host to an even numbered host.

4.4.1.4 About the Lifecycle 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.

It is recommended that the Lifecycle repository be mounted onto every host in the topology for the duration of provisioning. This allows the deployment process to place files into this location ready for use by other process steps that might be running on

different hosts. Having a centralized repository saves you from having to manually copy files around during the provisioning process.

Having a centralized repository is also important for patching. The repository is only required when provisioning or patching is occurring. At other times, this disk share can be unmounted from any or all hosts, ensuring security across zones is maintained.

The advantages of having a shared lifecycle repository are:

1. Single location for software.
2. Simplified deployment provisioning.
3. Simplified patching.

Some organizations may prohibit the mounting of file systems across zones, even if it is only for the duration of initial provisioning or for patching. In this case, when you undertake deployment provisioning, you must duplicate the software repository and perform a number of manual file copies during the deployment process.

For simplicity, this guide recommends using a single shared lifecycle repository. However the guide does include the necessary extra manual steps in case this is not possible.

4.4.2 Recommendations for Domain Configuration Files

The following sections describe guidelines for using shared storage for the Oracle WebLogic Server domain configuration files you create when you configure your Oracle Fusion Middleware products in an enterprise deployment:

- Section 4.4.2.1, "About Oracle WebLogic Server Administration and Managed Server Domain Configuration Files"
- Section 4.4.2.2, "Shared Storage Requirements for Administration Server Domain Configuration Files"
- Section 4.4.2.3, "Local Storage Requirements for Managed Server Domain Configuration Files"

4.4.2.1 About Oracle WebLogic Server Administration and Managed Server Domain Configuration Files

When you configure an Oracle Fusion Middleware product, you create or extend an Oracle WebLogic Server domain. Each Oracle WebLogic Server domain consists of a single Administration Server and one or more managed servers.

For more information about Oracle WebLogic Server domains, see *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server*.

In an enterprise deployment, it is important to understand that the managed servers in a domain can be configured for active-active high availability. However, the Administration server cannot. The Administration Server is a singleton service. That is, it can be active on only one host at any given time.

ASERVER_HOME is the primary location of the domain configuration. *MSERVER_HOME* is a copy of the domain configuration that is used to start and stop managed servers. The WebLogic Administration Server automatically copies configuration changes applied to the *ASERVER_HOME* domain configuration to all those *MSERVER_HOME* configuration directories that have been registered to be part of the domain. However, the *MSERVER_HOME* directories also contain deployments and data specific to the managed servers. For that reason, when performing backups, you must include both *ASERVER_HOME* and *MSERVER_HOME*.

4.4.2.2 Shared Storage Requirements for Administration Server Domain Configuration Files

Administration Server configuration files must reside on Shared Storage. This allows the administration server to be started on a different host should the primary host become unavailable. The directory where the administration server files is located is known as the *ASERVER_HOME* directory. This directory is located on shared storage and mounted to each host in the application tier.

Managed Server configuration Files should reside on local storage to prevent performance issues associated with contention. The directory where the managed server configuration files are located is known as the *MSERVER_HOME* directory. It is highly recommended that managed server domain configuration files be placed onto local storage.

4.4.2.3 Local Storage Requirements for Managed Server Domain Configuration Files

If you must use shared storage, it is recommended that you create a storage partition for each node and mount that storage exclusively to that node

The configuration steps provided for this enterprise deployment topology assume that a local domain directory for each node is used for each managed server.

4.4.3 Shared Storage Recommendations for JMS File Stores and Transaction Logs

JMS file stores and JTA transaction logs must be placed on shared storage in order to ensure that they are available from multiple hosts for recovery in the case of a server failure or migration.

For more information about saving JMS and JTA information in a file store, see "Using the WebLogic Persistent Store" in *Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server*.

4.4.4 Recommended Directory Locations

This section describes the recommended use of shared and local storage.

This section includes the following topics:

- Section 4.4.4.1, "Lifecycle Management and Deployment Repository"
- Section 4.4.4.2, "Shared Storage"
- Section 4.4.4.3, "Private Storage"

4.4.4.1 Lifecycle Management and Deployment Repository

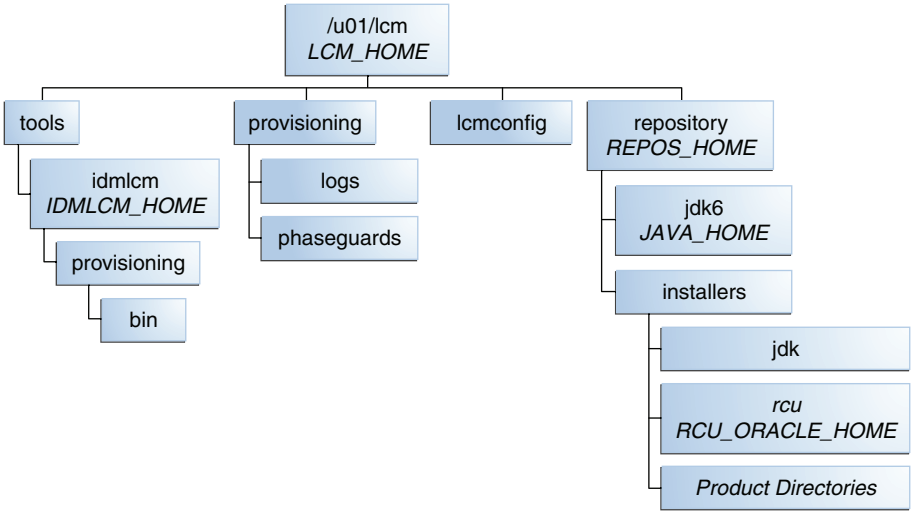
You need a separate share to hold the Lifecycle Management Tools and Deployment Repository. This share is only required during deployment and any subsequent patching. Once deployment is complete, you can unmount this share from each host.

> **Note:** 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 provisioning. Doing so will make the provisioning 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.

Figure 4–1 Deployment Repository



4.4.4.2 Shared Storage

In an Enterprise Deployment, it is recommended that the volume `VOL1/OracleIAM` be created on shared storage on hosts OAMHOST1, OAMHOST2, OIMHOST1, and OIMHOST2. The mount point must be `/u01/oracle`.

The recommended layout is described in Table 4–1 and Table 4–2 and shown in Figure 4–2.

> **Note:** Even though it is not shared, the *`IDM_TOP`* location must be writable.

Table 4–1 Volumes on Shared Storage–Distributed Topology

Environment Variable	Volume Name	Mount Point	Mounted on Hosts	Exclusive
SW_ROOT	Binaries	`/u01/oracle/products`	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2 LDAPHOST1 LDAPHOST2[1]	No
SHARED_ CONFIG_DIR	sharedConfig	`/u01/oracle/config`	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	No
DIR_MW_ HOME[2]	dirBinaries	`/u01/oracle/products/dir`	LDAPHOST1 LDAPHOST2	No

[1] Only mount to LDAPHOST1 and LDAPHOST2 when directory is in the Application Zone

[2] Only required when directory is being placed into a Directory/Database Zone

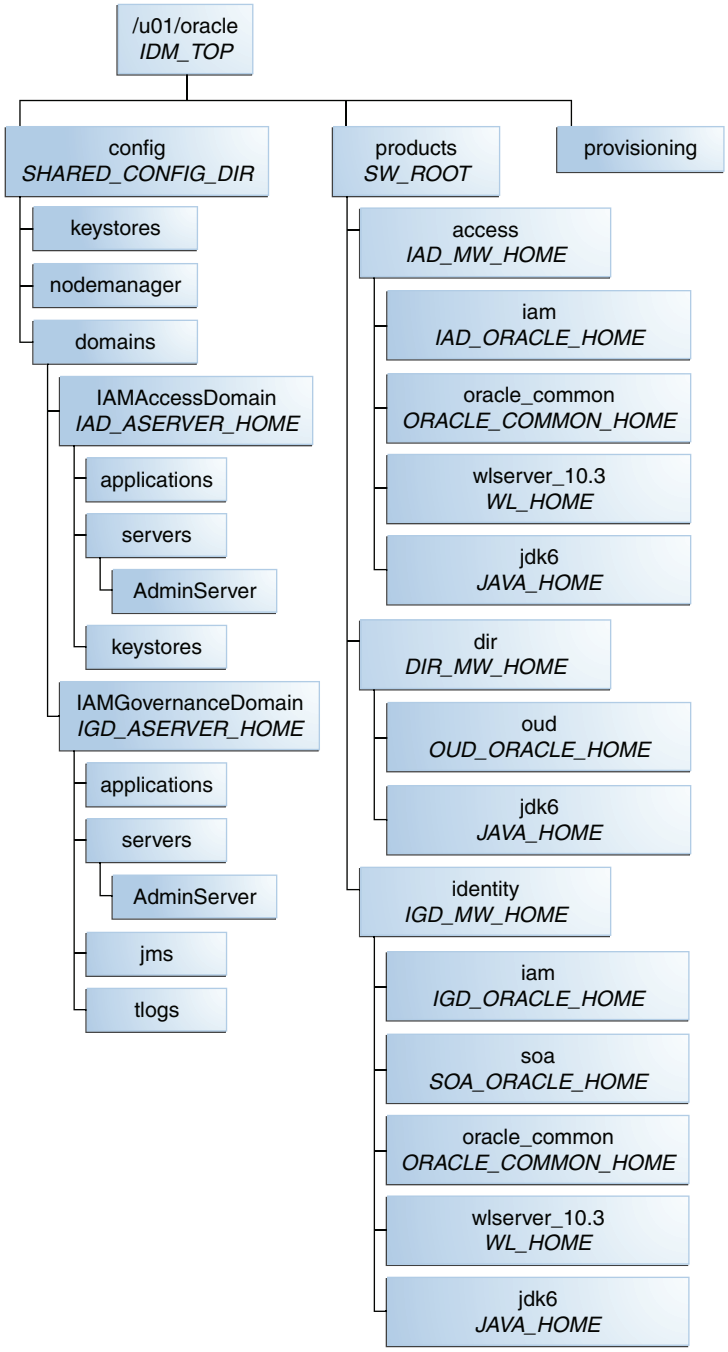
Table 4–2 Volumes on Shared Storage–Consolidated Topology

Environment Variable	Volume Name	Mount Point	Mounted on Hosts	Exclusive
SW_ROOT	Binaries	`/u01/oracle/products`	IAMHOST1 IAMHOST2 LDAPHOST1 LDAPHOST2[1]	No
SHARED_CONFIG_DIR	sharedConfig	`/u01/oracle/config`	IAMHOST1 IAMHOST2	No
DIR_MW_HOME[2]	dirBinaries	`/u01/oracle/products/dir`	LDAPHOST1 LDAPHOST2	No

[1] Only mount to LDAPHOST1 and LDAPHOST2 when directory is in the Application Zone

[2] Only required when directory is being placed into a Directory/Database Zone

Figure 4–2 Shared Storage



The figure shows the shared storage directory hierarchy. Under the mount point, `/u01/oracle` (*SW_ROOT*) are the directories `config` and `products`.

If you plan to deploy your directory into a different zone from the application tier and you do not want to mount your storage across zones, then you can create shared storage dedicated to the directory tier for the purposes of holding DIR_MW_HOME. Note that this will still have the same mount point as the shared storage in the application tier, for example: `/u01/oracle`.

The directory `config` contains `domains`, which contains:

- IAMAccessDomain (*IAD_ASERVER_HOME*). IAMAccessDomain has three subdirectories: applications, servers, and keystores. The servers directory has a subdirectory, AdminServer.
- IAMGovernanceDomain (*IGD_ASERVER_HOME*). IAMGovernanceDomain has five subdirectories: applications, servers, keystores, jms, and tlogs. The servers directory has a subdirectory, AdminServer.

The directory products contains the directories access, dir, and identity.

The directory access (*IAD_MW_HOME*) has four subdirectories: iam (*IAD_ORACLE_HOME*), oracle_common (*ORACLE_COMMON_HOME*), wlserver_10.3 (*WL_HOME*), and jdk6 (*JAVA_HOME*).

The directory dir (*DIR_MW_HOME*) has two subdirectories: oud (*OUD_ORACLE_HOME*) and jdk6(*JAVA_HOME*).

The directory identity (*IGD_MW_HOME*) has five subdirectories: iam (*IGD_ORACLE_HOME*), soa (*SOA_ORACLE_HOME*), oracle_common (*ORACLE_COMMON_HOME*), wlserver_10.3 (*WL_HOME*), and jdk6 (*JAVA_HOME*).

The directory provisioning is used by the Identity and Access Deployment Wizard and contains information relating to the deployment plan.

If you have a dedicated directory tier, the share for *SW_ROOT* will be different depending on whether or not you are on an LDAPHOST or an IAMHOST

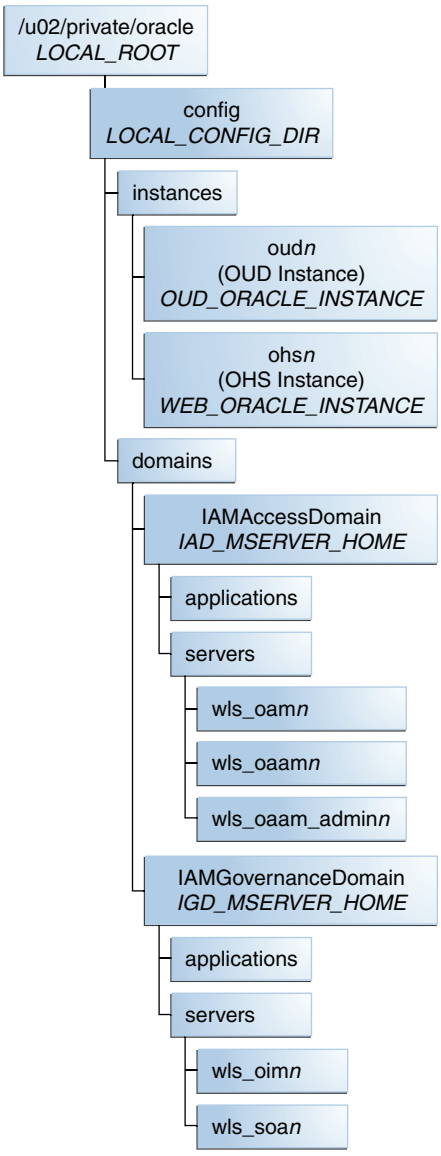
4.4.4.3 Private Storage

In an Enterprise Deployment it is recommended that the following directories be created on local storage or on shared storage mounted exclusively to a given host:

Table 4–3 Private Storage Directories

Tier	Environment Variable	Directory	Hosts
Web Tier	*WEB_MW_HOME*	/u01/oracle/products/web	WEBHOST1 WEBHOST2
Web Tier	*WEB_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/ohs*n*	WEBHOST1 WEBHOST2
Application Tier	*OUD_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oud*n*	LDAPHOST1 LDAPHOST2
	IAD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMAccessDomain	OAMHOST1 OAMHOST2
	IGD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMGovernanceDomain	OIMHOST1 OIMHOST2

Figure 4–3 Private Storage



The figure shows the local storage directory hierarchy. The top level directory, `/u02/private/oracle` (*`LOCAL_ROOT`*), has a subdirectory, `config`.

The directory `config` has a subdirectory for each product that has an instance, that is, Web Server and LDAP (in this case, Oracle HTTP Server and Oracle Unified Directory). The appropriate directory only appears on the relevant host, that is, the *`WEB_ORACLE_INSTANCE`* directory only appears on the WEBHOSTS

The `domains` directory contains one subdirectory for each domain in the topology, that is, `IAMAccessDomain` and `IAMGovernanceDomain`.

`IAMAccessDomain` (*`IAD_MSERVER_HOME`*) contains `applications` and `servers`. The `servers` directory contains `wls_oamn`, where *`n`* is the Access Manager instance. If OAAM is configured, this folder also contains `wls_oaamn` and `wls_oaam_adminn`

`IAMGovernanceDomain` (*`IGD_MSERVER_HOME`*), which contains `applications` and `servers`. The `servers` directory contains `wls_oimn` and `wls_soan`, where *`n`* is the Oracle Identity Manager and SOA instance, respectively.

Figure 4–4 Private Binary Storage

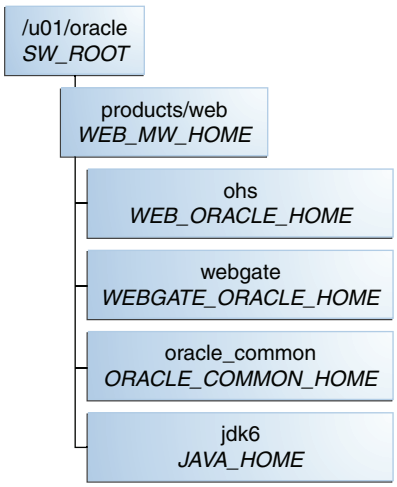


Figure 4–4 shows the local binary storage directory hierarchy. The top level directory, `/u01/oracle` (), has a subdirectory, `products`.

The `products` directory contains the `web` directory (*`WEB_MW_HOME`*), which has four subdirectories: `web` (*`WEB_ORACLE_HOME`*), `webgate` (*`WEBGATE_ORACLE_HOME`*), `oracle_common` (*`ORACLE_COMMON_HOME`*), and `jdk6` (*`JAVA_HOME`*).

Note: While it is recommended that you put *`WEB_ORACLE_INSTANCE`* directories onto local storage, you can use shared storage. If you use shared storage, you must ensure that the HTTP lock file is placed on discrete locations.

5

Configuring the Servers for an Enterprise Deployment

This chapter describes how to prepare the servers for an enterprise deployment.

It contains the following sections:

5.1 Overview of Configuring the Servers

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.

The settings described in this chapter are 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.

5.2 Verifying Your Server and Operating System

Ensure that the server and operating system that you plan to use is a certified combination for the products you plan to use. Refer to Oracle Certification Matrix for details.

5.3 Meeting the Minimum Hardware Requirements

In order to use a server in an Oracle Enterprise Deployment you must verify that it meets the minimum specification described in Section 2.4, "Hardware Requirements

for an Enterprise Deployment." If you plan to use a different deployment architecture, for example, one with more or fewer components deployed on a different number of boxes, you must check *Oracle® Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* to ensure that you have the minimum specification to support the products you plan to deploy on these servers.

If you are deploying to a virtual server environment, ensure that each of the virtual servers meets the minimum requirements.

Ensure that you have sufficient local disk and shared storage is configured as described in Chapter 4, "Preparing Storage for an Enterprise Deployment."

Allow sufficient swap and temporary space. Specifically:

- **Swap Space**–The system must have at least 512MB.
- **Temporary Space**–There must be a minimum of 500MB of free space in `/tmp`.

5.4 Meeting Operating System Requirements

Before performing Identity and Access Management Deployment, you must perform the following tasks:

1. Install a certified operating system.
2. Install all necessary patches and packages as listed in the Release Notes.

This section includes the following topics:

- Section 5.4.1, "Configure Kernel Parameters."
- Section 5.4.2, "Setting the Open File Limit."
- Section 5.4.3, "Setting Shell Limits."
- Section 5.4.4, "Configuring Local Hosts File."

5.4.1 Configure Kernel Parameters

The kernel parameter and shell limit values shown below are recommended values only. For production systems, Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

Kernel parameters must be set to a minimum of those below on all nodes in the topology.

The values in the following table are the current Linux recommendations. For the latest recommendations for Linux and other operating systems, see *Oracle Fusion Middleware System Requirements and Specifications*.

If you are deploying a database onto the host, you might need to modify additional kernel parameters. Refer to the 11*g* Release 2 *Oracle Grid Infrastructure Installation Guide* for your platform.

Table 5–1 UNIX Kernel Parameters

Parameter	Value
kernel.sem	256 32000 100 142
kernel.shmmax	2147483648 or higher

To set these parameters:

1. Log in as `root` and add or amend the entries in the file `/etc/sysctl.conf`.
2. Save the file.
3. Activate the changes by issuing the command:

```
/sbin/sysctl -p
```

5.4.2 Setting the Open File Limit

On all UNIX operating systems, the minimum Open File Limit should be 4096.

> **Note:** The following examples are for Linux operating systems. Consult your operating system documentation to determine the commands to be used on your system.

You can see how many files are open with the following command:

```
/usr/sbin/lsof | wc -l
```

To check your open file limits, use the commands below.

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

5.4.3 Setting Shell Limits

> **Note:** If your limits are already set higher than these values, you do not need to change them.

Most Linux Versions

To change the shell limits, login as `root` and edit the `/etc/security/limits.conf` file.

Add the following lines:

```
* soft  nofile  65536
* hard  nofile  150000
* soft  nproc   2048
* hard  nproc   16384
```

Oracle Linux 6 and Red Hat Enterprise Linux 6 Only

To change the shell limits, login as `root` and edit the `/etc/security/limits.conf` file.

Add the following lines:

```
* soft  nofile  65536
* hard  nofile  150000
```

Also edit: `/etc/security/limits.d/90-nproc.conf`

Add the following lines:

```
* soft  nproc   2048
* hard  nproc   16384
```

For the most recent suggested values, see *Oracle Fusion Middleware System Requirements and Specifications*.

After editing the file, reboot the machine.

5.4.4 Configuring Local Hosts File

Before you begin the installation of the Oracle software, ensure that your local `/etc/hosts` file is formatted like this:

```
IP_Address Fully_Qualified_Name Short_Name
```

For example

```
192.168.30.1 iamhost1.mycompany.com iamhost1
```

5.5 Enabling Unicode Support

Your operating system configuration can influence the behavior of characters supported by Oracle Fusion Middleware products.

On UNIX operating systems, Oracle highly recommends that you enable Unicode support by setting the `LANG` environment variable to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Oracle SOA Suite technologies, for example, are based on Unicode.

Set the LANGUAGE environment variable as follows:

```
LANG=en_GB.UTF-8
```

If the operating system is configured to use a non-UTF-8 encoding, Oracle SOA Suite components may function in an unexpected way. For example, a non-ASCII file name might make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

5.6 Enabling Virtual IP Addresses

The enterprise deployment requires that certain hosts, such as those running the WebLogic Administration Server or SOA managed servers, use virtual IP addresses. You must enable the appropriate IP address on each server.

Chapter 3, "Preparing the Network for an Enterprise Deployment" describes the mapping of IP Addresses to servers.

This section includes the following topics:

- Section 5.6.1, "Summary of the Required Virtual IP Addresses"
- Section 5.6.2, "Enabling a Virtual IP Address on a Existing Network Interface"
-

5.6.1 Summary of the Required Virtual IP Addresses

Virtual IP Addresses are required for failover of the WebLogic Administration Server, regardless of whether other Oracle Fusion Middleware components are installed later or not.

You associate the Administration Server with a virtual IP address. This allows the Administration Server to be started on a different host if the primary host fails.

Check that the virtual host is enabled as follows:

Table 5–2 Virtual Hosts for Domain

VIP	Enabled on Host (Distributed)	Enabled on Host (Consolidated)
IADADMINVHN.mycompany.com	OAMHOST1	IAMHOST1
IGDADMINVHN.mycompany.com	OIMHOST1	IAMHOST1
OIMHOST1VHN.mycompany.com	OIMHOST1	IAMHOST1
OIMHOST2VHN.mycompany.com	OIMHOST2	IAMHOST2
SOAHOST1VHN.mycompany.com	OIMHOST1	IAMHOST1
SOAHOST2VHN.mycompany.com	OIMHOST2	IAMHOST2

Note: This is the DNS name associated with the floating IP address. It is not the DNS name of the virtual host configured on the load balancer.

5.6.2 Enabling a Virtual IP Address on a Existing Network Interface

To enable only the physical IP addresses listed in Table 5–2, on IAMHOST1 and IAMHOST2:

1. Use the `ifconfig` command to create the virtual IP address:

   ```
   ifconfig subinterface virtual_ip_address netmask netmask_value
   ```

   For example, on IAMHOST1, enter the following:

   ```
   ifconfig bond0:1 192.168.20.3 netmask 255.255.240.0
   ```

2. For each virtual IP address you define, update the ARP caches using the following command:

   ```
   arping -b -A -c 3 -I bond0 192.168.20.3
   ```

5.7 Mounting Shared Storage onto the Host

As shown in Chapter 4, "Preparing Storage for an Enterprise Deployment," you must make shared storage available to each host that will use it.

5.7.1 Shared Storage Overview

Mount shared storage as follows:

Table 5–3 Mounting Shared Storage

Topology	Volume	Mount Point	Mounted on Hosts	Directory Tier	Temporary
Consolidated	`binaries`	`/u01/oracle/products`	IAMHOST1 IAMHOST2		No

Table 5–3 (Cont.) Mounting Shared Storage

Topology	Volume	Mount Point	Mounted on Hosts	Directory Tier	Temporary
	sharedConfig	u01/oracle/config	IAMHOST1 IAMHOST2 LDAPHOST1 LDAPHOST2	N/A	No
	LCM	/u01/lcm	WEBHOST1 WEBHOST2 IAMHOST1 IAMHOST2	N/A	Yes
Distributed	binaries	/u01/oracle/products	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2		No
	dirBinaries	/u01/oracle/products	LDAPHOST1 LDAPHOST2		No
	sharedConfig	/u01/oracle/config	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	N/A	No
	LCM	/u01/lcm	WEBHOST1 WEBHOST2 OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2 LDAPHOST1 LDAPHOST2	N/A	Yes

Note the following points:

- Each host must have appropriate privileges set within the NAS or SAN so that it can write to the shared storage.
- Temporary mounts are only required during provisioning and patching.
- If your directory tier is placed into a dedicated zone, you must share the ORACLE_BASE between the two directory hosts in a distributed topology.
- If WEBHOST1 and WEBHOST2 are in the DMZ, ORACLE_BASE is not shared between those two hosts.
- Follow the best practices of your organization for mounting shared storage. This section provides an example of how to do this on UNIX or Linux using NFS storage.

> **Note:** The user ID used to create a shared storage file system owns and has read, write, and execute privileges for those files. Other users in the operating system group can read and execute the files, but they do not have write privileges. For more information about installation and configuration privileges, see the "Understanding Installation and Configuration Privileges and Users" section in the *Oracle Fusion Middleware Installation Planning Guide*.

5.7.2 Mounting Shared Storage

You must create and mount shared storage locations so that each application tier host can see the same location for the binary installation.

You use the following command to mount shared storage from a NAS storage device to a linux host. If you are using a different type of storage device or operating system, refer to your manufacturer documentation for information about how to do this.

To mount shared storage on a host, use a command similar to the following:

```
mount -t nfs nasfiler:volume mountpoint
```

For example:

```
mount -t nfs nasfiler:VOL1/OracleIAM /u01/oracle
```

Where *nasfiler* is the name of the shared storage device.

Using the `mount` command as described mounts the shared storage until the host is rebooted. Once rebooted, the storage must be remounted to the host.

To ensure that storage is made available following a host reboot, place an entry into the file `/etc/fstab` which looks like the following:

```
nasfiler:VOL1/OracleIAM /u01/oracle nfs
auto,rw,bg,hard,nointr,proto=tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

Note: The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from OAMHOST1. The options may differ depending on the specific storage device.

```
mount -t nfs -o
rw,bg,hard,nointr,proto=tcp,vers=3,timeo=300,rsize=32768,wsize=3276
8 nasfiler:VOL1/OracleIAM /u01/oracle
```

Contact your storage vendor and machine administrator for the correct options for your environment.

5.7.3 Validating the Shared Storage Configuration

Ensure that you can read and write files to the newly mounted directories by creating a test file in the shared storage location you just configured.

For example:

```
cd /u01/oracle/products
touch testfile
```

Verify that the owner and permissions are correct:

```
ls -l testfile
```

Then remove the file:

```
rm testfile
```

5.8 Configuring Users and Groups

Create the following users and groups either locally or in your NIS or LDAP server. This user is the Oracle Software Owner.

The instructions below are for creating the users locally. Refer to your NIS documentation for information about creating these users/groups in your NIS server.

Groups

You must create the following groups on each node.

- `oinstall`
- `dba`

To create the groups, use the following command as root:

```
groupadd groupname
```

For example

```
groupadd -g 500 oinstall
groupadd -g 501 dba
```

Users

You must create the following users on each node.

- `oracle`–The owner of the Oracle software. You may use a different name. The primary group for this account must be `oinstall`. The account must also be in the `dba` group.

Notes:

- The group `oinstall` must have write privileges to all the file systems on shared and local storage that are used by the Oracle software.
- Each group must have the same Group ID on every node.
- Each user must have the same User ID on every node.
- The user and group should exists at the NIS server due to the NFSv4 mount requirement.

To create users use the following command as root:

```
useradd -g primary group -G optional groups -u userid username
```

For example:

```
useradd -g oinstall -G dba -u 500 oracle
```

6

Preparing the Database for an Enterprise Deployment

This chapter describes how to install and configure the Identity and Access Management database repositories.

This chapter contains the following topics:

6.1 Overview of Preparing the Databases for an Identity and Access Management Enterprise Deployment

The Identity and Access Management components in the enterprise deployment use database repositories. This chapter describes how to perform the following steps:

- Verify the database requirements as described in Section 6.2, "Verifying the Database Requirements for an Enterprise Deployment."
- Install and configure the Oracle database repositories. See the installation guides listed in the "Related Documents" section of the Preface and Section 6.3, "Installing the Database for an Enterprise Deployment."
- Create database services, as described in Section 6.4, "Creating Database Services."
- Prepare the database for the Repository Creation Utility (RCU). See Section 7.2, "Creating an Oracle Identity and Access Management Software Repository."
- Create the required Oracle schemas in the database using the Repository Creation Utility (RCU). See Section 6.5, "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU."

6.2 Verifying the Database Requirements for an Enterprise Deployment

Before loading the metadata repository into your databases, check that they meet the requirements described in these subsections:

6.2.1 Databases Required

For Oracle Identity and Access Management, a number of separate databases are recommended. Table 6–1 provides a summary of these databases. Which database or databases you use depends on the topology that you are implementing.

The Oracle Metadata Services (MDS) Repository is a particular type of repository that contains metadata for some Oracle Fusion Middleware components. It can also include custom Java EE applications developed by your organization.

For this release of IAM you must use a separate RCU schema prefix each domain. This allows different products to use a different database if required.

Table 6–1 Mapping between Databases and Schemas

Database Names	Database Hosts	Scan Address	Service Names	RCU Prefix	Schemas in Database
IAMDB	IAMDBHOST1 IAMDBHOST2	*IAMDBSCAN*	`OAMEDG.mycompany.com`	EDGIAD	OAM, IAU, MDS, OPSS
			`OIMEDG.mycompany.com`	EDGIGD	OIM, SOAINFRA, MDS, OPSS, ORASDPM
			`OAAMEDG.mycompany.com`	EDGIAD	OAAM

The following sections apply to all the databases listed in Table 6–1.

6.2.2 Database Host Requirements

The database used to store the metadata repository should be highly available in its own right, for maximum availability Oracle recommends the use of an Oracle Real Application Clusters (RAC) database.

Ideally the database should use Oracle Automatic Storage Management (ASM) for the storage of data, however this is not necessary.

If using ASM, then ASM should be installed into its own Oracle home and have two disk groups:

- One for the Database Files
- One for the Flash Recovery Area

If you are using Oracle ASM, best practice is to also use Oracle Managed Files.

6.2.3 Database Versions Supported

The Deployment Tools require that you have Oracle Database 11.2.0.0 or newer for Oracle RAC deployments.

To check if your database is certified or to see all certified databases, refer to the "Certified Databases" section in the Certification Document:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

To determine the version of your installed Oracle Database, execute the following query at the SQL prompt:

```
select version from sys.product_component_version where product like 'Oracle%';
```

6.2.4 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

If you are using Oracle Database 11*g* (11.2.0.2.0), make sure that you download and install the appropriate version (based on the platform) for the RDBMS Patch Number 10259620. This is a prerequisite for installing the Oracle Identity Manager schemas.

Table 6–2 lists the patches required for Oracle Identity Manager configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 6–2 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit) Linux x86 (64-bit)	RDBMS Interim Patch#10259620.

If this patch is not applied, then problems might occur in user and role search and manager lookup. In addition, search results might return empty result.

Note:

- Apply this patch in ONLINE mode. Refer to the readme.txt file bundled with the patch for the steps to be followed.
- In some environments, the RDBMS Interim Patch has been unable to resolve the issue, but the published workaround works. Refer to the note "Wrong Results on 11.2.0.2 with Function-Based Index and OR Expansion due to fix for Bug:8352378 [Metalink Note ID 1264550.1]" at http://support.oracle.com for the workaround. This note can be followed to set the parameters accordingly with the only exception that they need to be altered at the Database Instance level by using ALTER SYSTEM SET <param>=<value> scope=<memory> or <both>.

6.2.5 Oracle Database Minimum Requirements

The Oracle Database must meet some minimum requirements.

6.2.5.1 General Database Characteristics

- Character Set–The character set must be Unicode compliant, for example: AL32UTF8.
- Database Options–The following database options must be installed into the database:
  - Oracle JVM
  - Oracle Text

- Database Views–The following Database view must be created on the database:
  - XAVIEWS
- Database Packages–The following Database package must exist in the database:
  - DBMS_SHARED_POOL

6.2.5.2 Minimum Initialization Parameters

The databases must have the following minimum initialization parameters defined:

Table 6–3 Minimum Initialization Parameters for Oracle Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	1600
session_max_open_files	50
sessions	500
processes	500
sga_target	512M
pga_aggregate_target	100M
sga_max_size	4G
session_cached_cursors	500

It is recommended that you set these parameters in the database configuration assistant when creating the database. If you have not done this, you can adjust them after creation by using the `alter system` database command. For example:

```
sqlplus / as sysdba
alter system set aq_tm_processes=1 scope=spfile;
```

After making changes in the `spfile`, restart the database. For example

```
srvctl stop database -d iamdb
srvctl start database -d iamdb
```

> **Note:** For guidelines on setting up optimum parameters for the Database, see *Oracle Fusion Middleware Performance and Tuning Guide*.

6.3 Installing the Database for an Enterprise Deployment

Install and configure the database repository as follows.

Oracle Clusterware

- For 10*g* Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in "Related Documents".
- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in "Related Documents".
- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.
- When you run the installer, select the **Configure Automatic Storage Management** option in the **Select Configuration** screen to create a separate Automatic Storage Management home.

Oracle Real Application Clusters

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in "Related Documents".
- For 11*g* Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

Oracle Real Application Clusters Database

Create a Real Applications Clusters Database with the following characteristics:

- Database must be in archive log mode to facilitate backup and recovery.
- Optionally, enable the Flashback database.
- Create UNDO tablespace of sufficient size to handle any rollback requirements during the Oracle Identity Manager reconciliation process.
- Database is created with ALT32UTF8 character set.

6.4 Creating Database Services

This section describes how to configure the database for Oracle Fusion Middleware 11g metadata. It contains the following topics:

- Section 6.4.1, "Creating Database Services for 10.x and 11.1.x Databases"
- Section 6.4.2, "Creating Database Services for 11.2.x Databases"
- Section 6.4.3, "Database Tuning"

6.4.1 Creating Database Services for 10.x and 11.1.x Databases

For complete instructions on creating database services, see the chapter on Workload Management in the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*. Oracle recommends that a specific database service be used for a product suite, even when product suites share the same database. It is also recommended that the database service used is different than the default database service.

Use the `CREATE_SERVICE` subprogram to create the database services for the components in your topology. The lists of services to be created are listed in Table 6–1, " Mapping between Databases and Schemas".

1. Log on to SQL*Plus as the `sysdba` user by typing:

   ```
   sqlplus "sys/password as sysdba"
   ```

   Then run the following command to create a service called `OAMEDG.mycompany.com` for Access Manager:

```
EXECUTE DBMS_SERVICE.CREATE_SERVICE
(SERVICE_NAME => 'OAMEDG.mycompany.com',
NETWORK_NAME => 'OAMEDG.mycompany.com');
```

2. Add the service to the database and assign it to the instances using srvctl:

```
srvctl add service -d iamdb -s OAMEDG.mycompany.com -r iamdb1,iamdb2
```

3. Start the service using `srvctl`:

```
srvctl start service -d iamdb -s OAMEDG.mycompany.com
```

6.4.2 Creating Database Services for 11.2.x Databases

Use `srvctl` to create the database services for the components in your topology. The lists of services to be created are listed in Table 6–1, " Mapping between Databases and Schemas".

1. Create service using the command `srvctl add service`, as follows.

```
srvctl add service -d iamdb -s OAMEDG.mycompany.com -r iamdb1,iamdb2 -q FALSE
-m NONE -e SELECT -w 0 -z 0
```

The meanings of the command-line arguments are as follows:

Option	Argument
-d	Unique name for the database
-s	Service name
-r	Comma separated list of preferred instances
-q	AQ HA notifications (TRUE or FALSE)
-e	Failover type (NONE, SESSION, or SELECT)
-m	Failover method (NONE or BASIC)
-w	Failover delay (integer)
-z	Failover retries (integer)

2. Start the Service using `srvctl start service`

```
srvctl start service -d iamdb -s OAMEDG.mycompany.com
```

3. Validate the service started by using `srvctl status service`, as follows:

```
srvctl status service -d iamdb -s OAMEDG.mycompany.com
Service OAMEDG.mycompany.com is running on instance(s) iamdb1,iamdb2
```

4. Validate that the service was created correctly by using `srvctl config service`:

```
srvctl config service -d iamdb -s OAMEDG.mycompany.com
Service name: OAMEDG.mycompany.com
Service is enabled
Server pool: IAMDB_OAMEDG.mycompany.com
Cardinality: 2
Disconnect: false
Service role: PRIMARY
Management policy: AUTOMATIC
DTP transaction: false
AQ HA notifications: false
```

```
Failover type: SELECT
Failover method: NONE
TAF failover retries: 0
TAF failover delay: 0
Connection Load Balancing Goal: LONG
Runtime Load Balancing Goal: NONE
TAF policy specification: NONE
Edition:
Preferred instances: iamdb1,iamdb2
Available instances:
```

Note: For more information about the SRVCTL command, see the *Oracle Real Application Clusters Administration and Deployment Guide*.

6.4.3 Database Tuning

The database parameters defined in Section 6.2.5.2, "Minimum Initialization Parameters" are only a guide. You might need to perform additional tuning after the system is in use. For more information, see *Database Performance Tuning Guide*.

Refresh the database statistics after you initially load the database, and on an ongoing basis. To do that, issue a SQL*Plus command for each schema. The following example is for the schema EDGIGD_OIM:

```
exec DBMS_STATS.GATHER_SCHEMA_STATS(OWNNAME=> 'EDGIGD_OIM', ESTIMATE_
PERCENT=>DBMS_STATS.AUTO_SAMPLE_SIZE, DEGREE=>8, OPTIONS=>'GATHER AUTO', NO_
INVALIDATE=>FALSE);
```

6.5 Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU

You must run the Repository Creation Utility to seed your database(s) with the schemas required for Identity and Access Management. You need to run the Repository Creation Utility twice, once for each domain specifying a different Prefix each time.

1. Start RCU by issuing this command:

   RCU_HOME/bin/rcu &

2. On the Welcome screen, click **Next**.
3. On the Create Repository screen, select the **Create** operation to load component schemas into a database. Then click **Next**.
4. On the Database Connection Details screen, provide the information required to connect to an existing database. For example:

   Database Type: `Oracle Database`

   - **Host Name:** Enter the VIP address of one of the RAC database nodes or the database SCAN address, for example: `IAMDBSCAN.mycompany.com`
   - **Port:** The port number for the database listener *(DB_LSNR_PORT)*. For example: `1521`
   - **Service Name:** The service name of the database. For example `OAMEDG.mycompany.com`.

Use the service names for the components you will select from the table in Step 6.

- **Username:** `sys`
- **Password:** The sys user password
- **Role:** `SYSDBA`

Click **Next**.

5. On the Check Prerequisites screen, click `OK` after the prerequisites have been validated.
6. On the Select Components screen, provide the following values:

   Create a New Prefix: Enter a prefix to be added to the database schemas. Note that all schemas are required to have a prefix. See Table 6–1, " Mapping between Databases and Schemas" or the following table for RCU prefixes.

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

RCU Prefix	Product	RCU Option	Service Name	Comments
EDGIAD	Oracle Platform Security Services for IAMAccessDomain	AS Common Schemas–Oracle Platform Security Service	`OAMEDG.mycompany.com`	Required to hold policy store information.
EDGIAD	Oracle Access Management Access Manager	Oracle Identity Management–Oracle Access Manager	`OAMEDG.mycompany.com`	Audit Services will also be selected.
EDGIAD	Oracle Adaptive Access Manager	Oracle Identity Management–Oracle Adaptive Access Manager	`OAAMEDG.mycompany.com`	If required.
EDGIGD	Oracle Platform Security Services for IAMGovernanceDomain	AS Common Schemas–Oracle Platform Security Service	`OIMEDG.mycompany.com`	Required to hold policy store information.
EDGIGD	Oracle Identity Manager	Identity Management–Oracle Identity Manager	`OIMEDG.mycompany.com`	Metadata Services, SOA infrastructure, and User Messaging will also be selected.

   Click **Next**.

   Notes: If your topology requires more than one database, the following important considerations apply:

   - Be sure to install the correct schemas in the correct database.
   - You might have to run the RCU more than once to create all the schemas for a given topology.
   - Table 6–1 in this chapter provides the recommended mapping between the schemas and their corresponding databases. Refer to this table to ensure that the correct details are entered in this screen.

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.

8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. The deployment wizard requires that all passwords for a given prefix be the same.

   Click **Next**.

9. On the Map Tablespaces screen, accept the defaults and click **Next**.
10. On the confirmation screen, click **OK** to allow the creation of the tablespaces.
11. On the Creating tablespaces screen, click OK to acknowledge creation of the tablespaces.
12. On the Summary screen, the summary and verify that the details provided are accurate. Click **Create** to start the schema creation process.
13. On the Completion summary screen, verify that the schemas were created.

    Click **Close** to exit.

6.6 Backing up the Database

After you have prepared your database, back it up as described in Section 15.5.3.3, "Backing Up the Database."

7

Preparing for Deployment

This chapter describes the software installations required for an Oracle Identity and Access Management enterprise deployment.

This chapter contains the following topics:

- Section 7.1, "Assembling Information for Identity and Access Management Deployment"
- Section 7.2, "Creating an Oracle Identity and Access Management Software Repository"
- Section 7.3, "Verifying Java"
- Section 7.4, "Installing the IAM Deployment Wizard"
- Section 7.5, "Checking Port Availability"

7.1 Assembling Information for Identity and Access Management Deployment

Assemble the following information prior to deployment. You can print out the tables from the PDF version of this guide and record your own values.

This guide repeatedly uses the following host names to make it easier to follow:

- WEBHOST1/2
- OAMHOST1/2
- OIMHOST1/2
- LDAPHOST1/2

The actual values you use depend on the type of deployment topology you are using. The values in Table 7–1 are translations of how these hosts refer to the hosts listed in the topologies.

In addition to the host names, you may see some of the hosts in the document have a VHN suffix. This is used to identity virtual host names.

Notes:

- Do not use host names that contain the hyphen (-) character. See Section 15.10.1.1, "Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute."
- Do not use privileged ports (< 1024) for the Identity and Access Management deployment.

Table 7–1 Hosts–Distributed Topology

Description	Variable	Documented Value	Customer Value
Access Management Host 1	*OAMHOST1*	OAMHOST1.mycompany.com	
Access Management Host 2	*OAMHOST2*	OAMHOST2.mycompany.com	
Identity Governance Host 1	*OIMHOST1*	OIMHOST1.mycompany.com	
Identity Governance Host 2	*OIMHOST2*	OIMHOST2.mycompany.com	
Directory Host 1	*LDAPHOST1*	LDAPHOST1.mycompany.com	
Directory Host 2	*LDAPHOST2*	LDAPHOST2.mycompany.com	
First Web Tier host	*WEBHOST1*	WEBHOST1.mycompany.com	
Second Web Tier host	*WEBHOST2*	WEBHOST2.mycompany.com	

Table 7–2 Hosts–Consolidated Topology

Description	Variable	Documented Value	Customer Value
Access Management Host 1	*OAMHOST1*	IAMHOST1.mycompany.com	
Access Management Host 2	*OAMHOST2*	IAMHOST2.mycompany.com	
Identity Governance Host 1	*OIMHOST1*	IAMHOST1.mycompany.com	
Identity Governance Host 2	*OIMHOST2*	IAMHOST2.mycompany.com	
Directory Host 1	*LDAPHOST1*	IAMHOST1.mycompany.com	
Directory Host 2	*LDAPHOST2*	IAMHOST2.mycompany.com	
First Web Tier host	*WEBHOST1*	IAMHOST1.mycompany.com	
Second Web Tier host	*WEBHOST2*	IAMSHOST2.mycompany.com	

Table 7–3 Installation Locations

Description	Variable	Documented Value	Customer Value
Software Repository Location	*REPOS_HOME*	/u01/lcm/repository	
Software Installation Location	*SW_ROOT*	/u01/oracle/products	
Shared Configuration Location	*SHARED_CONFIG_DIR*	/u01/oracle/config	
Local Configuration Location	*LOCAL_CONFIG_DIR*	/u02/private/oracle/config	
Lifecycle Management Store Location	*LCM_HOME*	/u01/lcm	

Table 7–4 Ports

Description	Variable	Documented Value	Customer Value
Access Management WLS Server Port	*IAD_WLS_PORT*	7001	
Identity Governance WLS Port	*IGD_WLS_PORT*	7101	
Oracle Identity Manager Port, Second Oracle Identity Manager Port	*OIM_PORT*	14000	
SOA Ports, Hosts 1 and 2	*SOA_PORT*	8001	
Access Manager Port, Second Access Manager Port	*OAM_PORT*	14100	
Access Manager Proxy Port	*OAM_PROXY_PORT*	5575	
Web Server HTTP Port	*WEB_HTTP_PORT*	7777	
Web Server HTTPS Port	*WEB_HTTPS_PORT*	4443	
LDAP Port	*LDAP_PORT*	1389	
LDAP SSL Port	*LDAP_SSL_PORT*	1636	
LDAP Administration Port	*LDAP_ADMIN_PORT*	4444	
LDAP Replication Port	*LDAP_REPLIC_PORT*	8989	
Node Manager Port	*NMGR_PORT*	5556	
OAAM Port	*OAAM_PORT*	14300	
OAAM Administration Port	*OAAM_ADMIN_PORT*	14200	

Table 7–5 Virtual Hosts

Description	Variable	Documented Value	Customer Value
Access Domain Administration Server Virtual Host	*IADADMINVHN*	IADADMINVHN.mycompany.com	
Governance Domain Administration Server Virtual Host	*IGDADMINVHN*	IGDADMINVHN.mycompany.com	
First Oracle Identity Manager Server virtual host	*OIMHOST1VHN*	OIMHOST1VHN.mycompany.com	
Second Oracle Identity Manager Server virtual host	*OIMHOST2VHN*	OIMHOST2VHN.mycompany.com	
First SOA Server virtual host	*SOAHOST1VHN*	SOAHOST1VHN.mycompany.com	
Second SOA Server virtual host	*SOAHOST2VHN*	SOAHOST2VHN.mycompany.com	

Table 7–6 Database Information

Description	Variable	Documented Value	Customer Value
SCAN Address	*SCAN_ADDRESS*	IAMDBSCAN.mycompany.com	
SCAN Listener Port	*DB_LSNR_PORT*	1521	
Oracle Identity Manager DB Service Name	*OIM_DB_SERVICENAME*	OIMEDG.mycompany.com	
Access Manager DB Service Name	*OAM_DB_SERVICENAME*	OAMEDG.mycompany.com	
OAAM DB Service Name	*OAAM_DB_SERVICENAME*	OAAMEDG.mycompany.com	
Oracle Identity Manager DB Schema Password	*OIM_SCHEMA_PASSWD*		

Table 7–7 LDAP

Description	Variable	Documented Value	Customer Value
LDAP Realm DN,	*REALM_DN*	dc=mycompany,dc=com	
Identity Store Bind DN	*LDAP_ADMIN_USER*	cn=oudadmin	

Table 7–8 Load Balancer

Description	Variable	Documented Value	Customer Value
Load Balancer end point used to access the IAMAccessDomain Administration functions	*IAD_DOMAIN_ADMIN_LBRVHN*	IADADMIN.mycompany.com	
Load Balancer end point used to access the IAMGovernanceDomain Administration functions	*IGD_DOMAIN_ADMIN_LBRVHN*	IGDADMIN.mycompany.com	
Load Balancer Administration Port	*HTTP_PORT*	80	
Load Balancer Administration Port is SSL?		No	
Load Balancer Internal Callbacks Virtual Host Name	*IAM_INTERNAL_LBRVHN*	IDMINTERNAL.mycompany.com	
Load Balancer Internal Callbacks Port	*IAM_INTERNAL_PORT*	80	
Load Balancer SSL Port	*HTTP_SSL_PORT*	443	
Load Balancer ID Store Virtual Host Name	*LDAP_IDSTORE_NAME*	IDSTORE.mycompany.com	
Load Balancer ID Store Port	*LDAP_LBR_PORT*	389	
Load Balancer ID Store SSL Port	*LDAP_LBR_SSL_PORT*	1636	
SSO main application entry point	*IAM_LOGIN_LBRVHN*	SSO.mycompany.com	

Table 7–9 Email Server (Optional)

Description	Variable	Documented Value	Customer Value
Outgoing Email Server Name	*EMAIL_SERVER*	EMAIL.mycompany.com	
Outgoing Email Server Port	*EMAIL_PORT*	465	
Outgoing Email Security	*EMAIL_PROTOCOL*	SSL	
Email Username	*EMAIL_USER*		
Email Password	*EMAIL_PASSWORD*		

Note: Internal call backs are always unencrypted (HTTP). The main entry point `sso.mycompany.com` is always encrypted (HTTPS)

Table 7–10 Users

Description	Variable	Documented Value	Customer Value
Common IAM Password for IAM Deployment Wizard	*COMMON_IAM_PASSWORD*		
Identity Store Access Manager Administrative User	*OAMADMINUSER*	oamadmin	
Identity Store Access Manager Software User	*OAMLDAPUSER*	oamLDAP	
Identity Store Oracle Identity Manager Administrative User	*OIMLDAPUSER*	oimLDAP	

Table 7–11 OAM

Description	Variable	Documented Value	Customer Value
Access Manager Transfer Mode	*OAM_MODE*	Simple. (Open on AIX.)	
Access Manager Cookie Domain	*OAM_COOKIE_DOMAIN*	.mycompany.com	

7.2 Creating an Oracle Identity and Access Management Software Repository

The software required by Oracle Identity and Access Management is located in the Oracle Fusion Middleware Deployment Repository. If you have not already done so then you must create an Oracle Fusion Middleware Provisioning Repository as described in *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

If you have not already done so, unzip the RCU zip file *REPOS_HOME*/installers/fmw_rcu/linux/rcuHome.zip to:

REPOS_HOME/installers/rcu

7.3 Verifying Java

Make sure that your Deployment Repository contains Java. It should reside in a directory called jdk6.

You can verify that Java is installed and working as follows:

Set JAVA_HOME to: *JAVA_HOME*

Run these commands:

```
JAVA_HOME/bin/java -version
JAVA_HOME/bin/javac -version
```

7.4 Installing the IAM Deployment Wizard

The IAM Deployment Wizard must be visible to each host in the topology during provisioning and subsequent patching.

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

REPOS_HOME/installers/idmlcm/Disk1

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

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

Then proceed as follows:

1. On the Welcome screen, click **Next**.
2. If you are running the Wizard on a UNIX platform, you are prompted for the location of the **Inventory Directory**, which is used to keep track of all Oracle products installed on this host.

   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 script.

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

   Click **OK** to continue.
3. On the Prerequisite Checks screen, verify that checks complete successfully, then click **Next**.
4. On the Specify Install Location screen, enter the following information:
   a. Oracle Middleware Home - This is the parent directory of the directory where the Identity and Access Management Deployment Wizard will be installed. This must be on shared storage for example:

      /u01/lcm/tools

   b. Oracle Home Directory - This is a subdirectory of the above directory where the wizard will be installed. For example:

      idmlcm

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

7.5 Checking Port Availability

Before starting to deploy your environment, you must ensure that none of the ports you intend to use is already in use.

To do this, perform the following steps:

1. Log on to the machine that the component will run on.
2. Check that no process is running using that port using the command:

   ```
   netstat -an | grep port
   ```

   where *port* is the port number you are checking for.

   For example, for Oracle HTTP server the command is:

   ```
   netstat -an | grep 7777
   ```

For a full list of the default ports, see Chapter 3–3, " Ports Used in the Oracle Identity and Access Management Enterprise Deployment Topology."

8

Creating a Deployment Profile

This chapter describes how to create a Deployment profile by using the Identity and Access Management Deployment Wizard.

This chapter describes the following wizard screens:

- Section 8.1, "Welcome."
- Section 8.2, "IAM Installation Options."
- Section 8.3, "Specify Security Updates."
- Section 8.4, "Describe Response File."
- Section 8.5, "Select IAM Products."
- Section 8.6, "Select Topology."
- Section 8.7, "Select Installation and Configuration Locations."
- Section 8.8, "Configure Virtual Hosts."
- Section 8.9, "Set User Names and Passwords."
- Section 8.10, "Configure Oracle Unified Directory."
- Section 8.11, "Configure Oracle HTTP Server."
- Section 8.12, "Configure Oracle Identity Manager."
- Section 8.13, "Configure Oracle Identity Manager Database."
- Section 8.14, "Configure SOA."
- Section 8.15, "Configure Oracle Access Manager."
- Section 8.16, "Configure Oracle Access Manager Database."
- Section 8.17, "Configure HTTP/HTTPS Load Balancer."
- Section 8.18, "Summary."

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

Refer to the information you assembled in Section 7.1, "Assembling Information for Identity and Access Management Deployment." Variable names used in the screen descriptions in this chapter were introduced in that section.

To start the Identity and Access Management Deployment Wizard, execute the following commands from: *IDMCLM*/provisioning/bin

Set JAVA_HOME to *REPOS_HOME*/jdk6.

Issue the command:

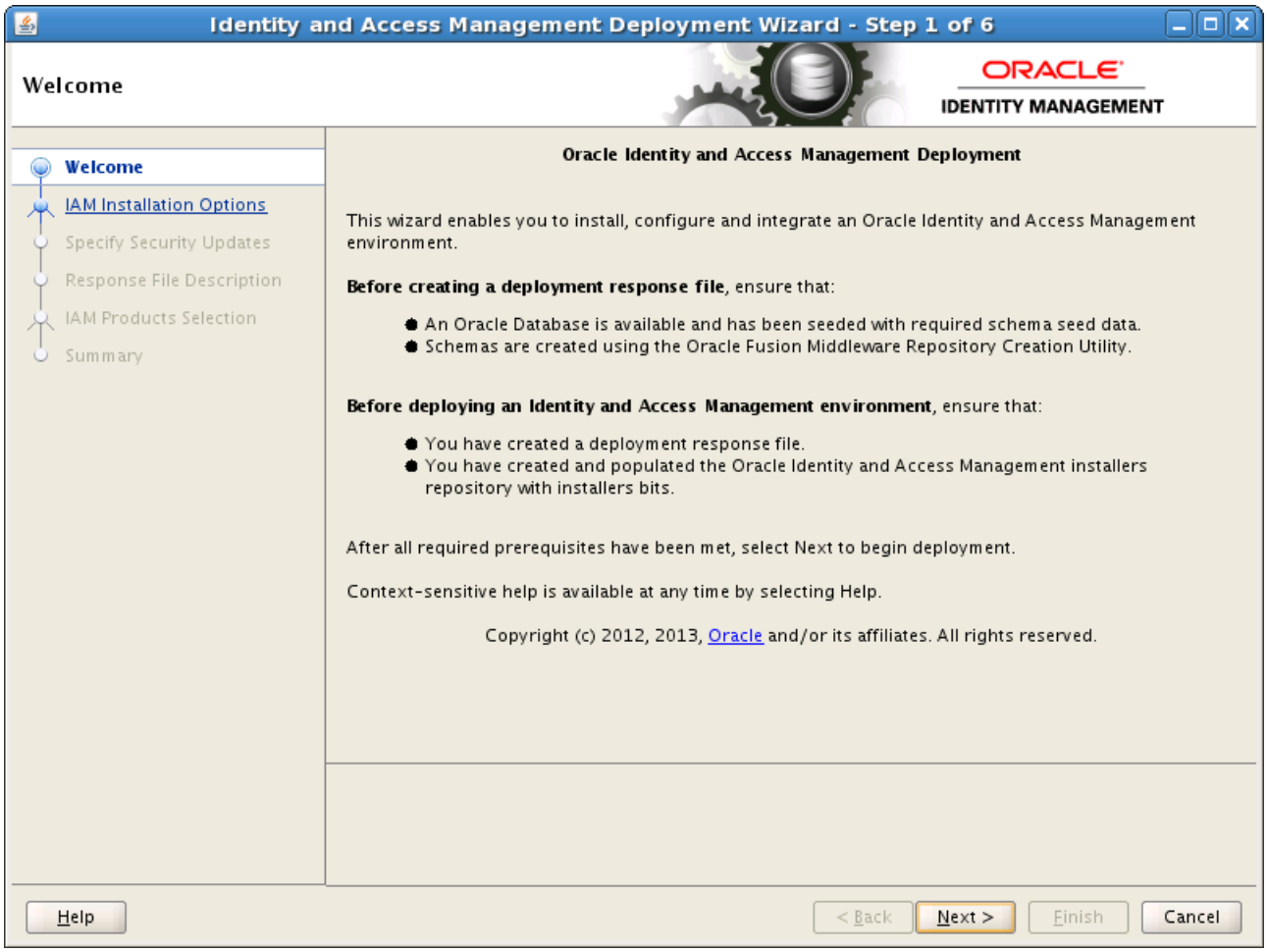
```
./iamDeploymentWizard.sh
```

When the wizard starts, proceed through the screens as described in the following subsections.

Note: The Identity and Access Management process requires that you use the same deployment profile on all hosts in the deployment. Create the deployment profile only once during the deployment process.

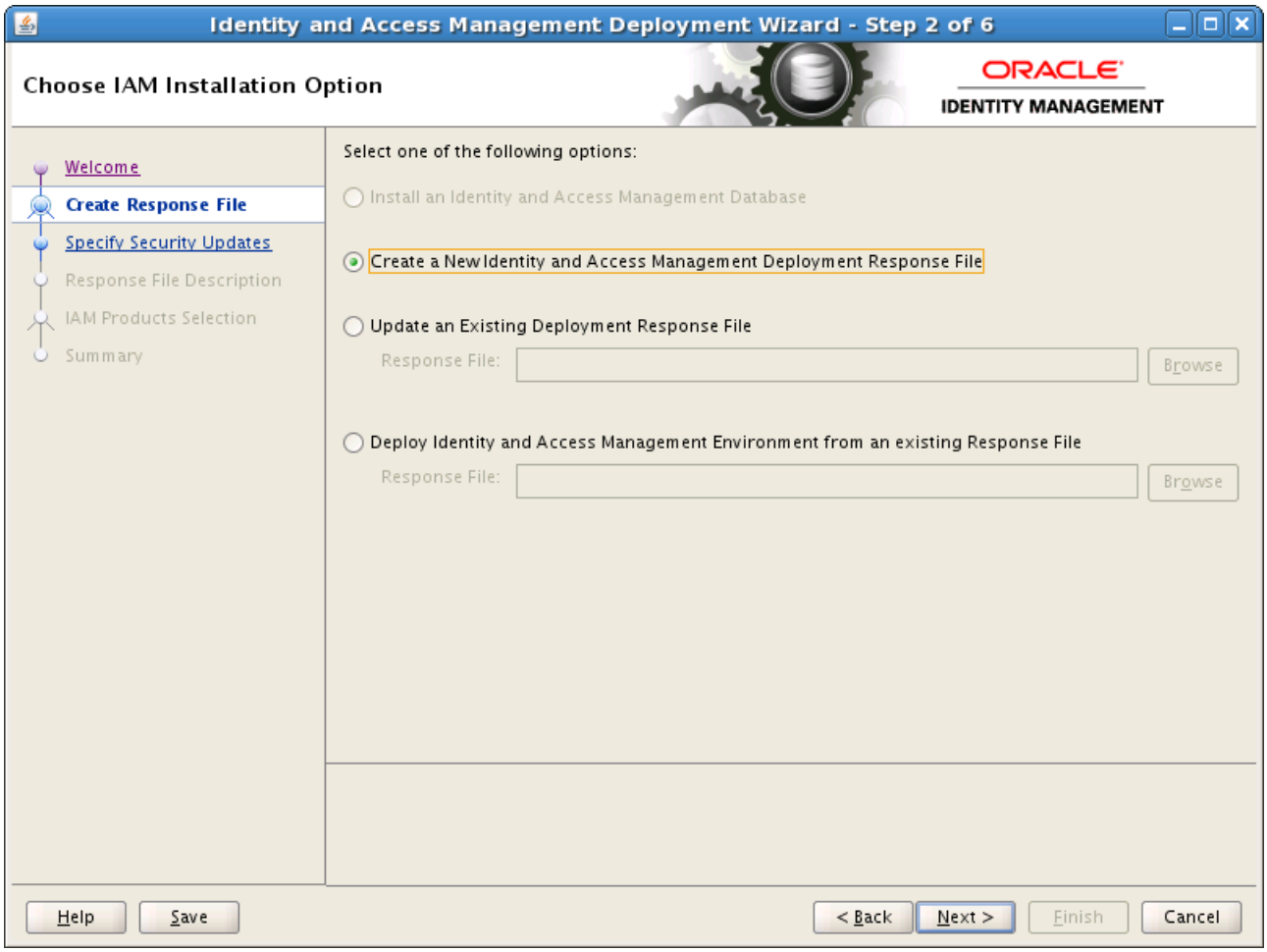
8.1 Welcome

On the Welcome screen, click **Next**.



8.2 IAM Installation Options

On the IAM Installation Options screen, select **Create a New Identity and Access Management Deployment Response File**, and click **Next**.

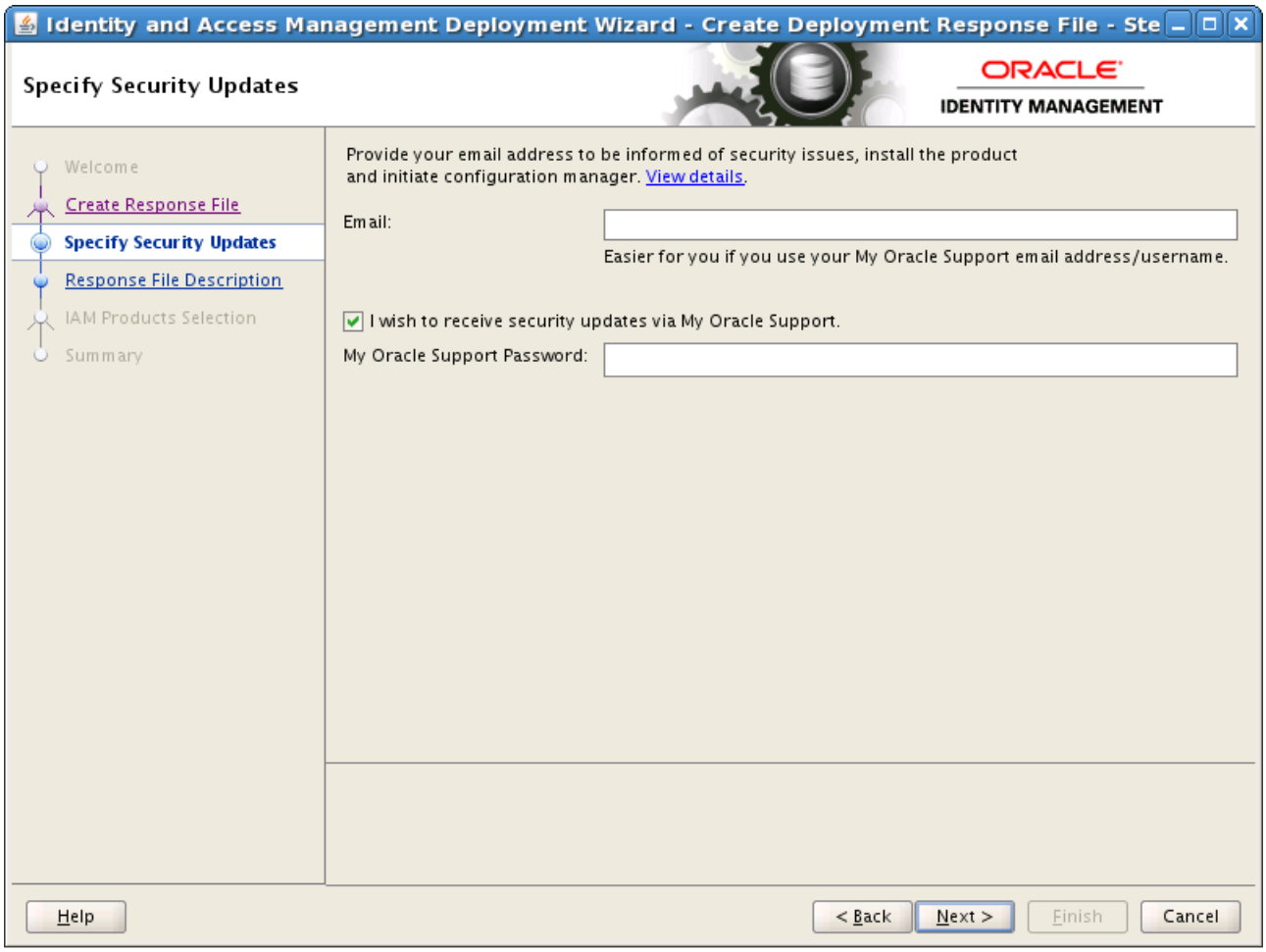


8.3 Specify Security Updates

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.

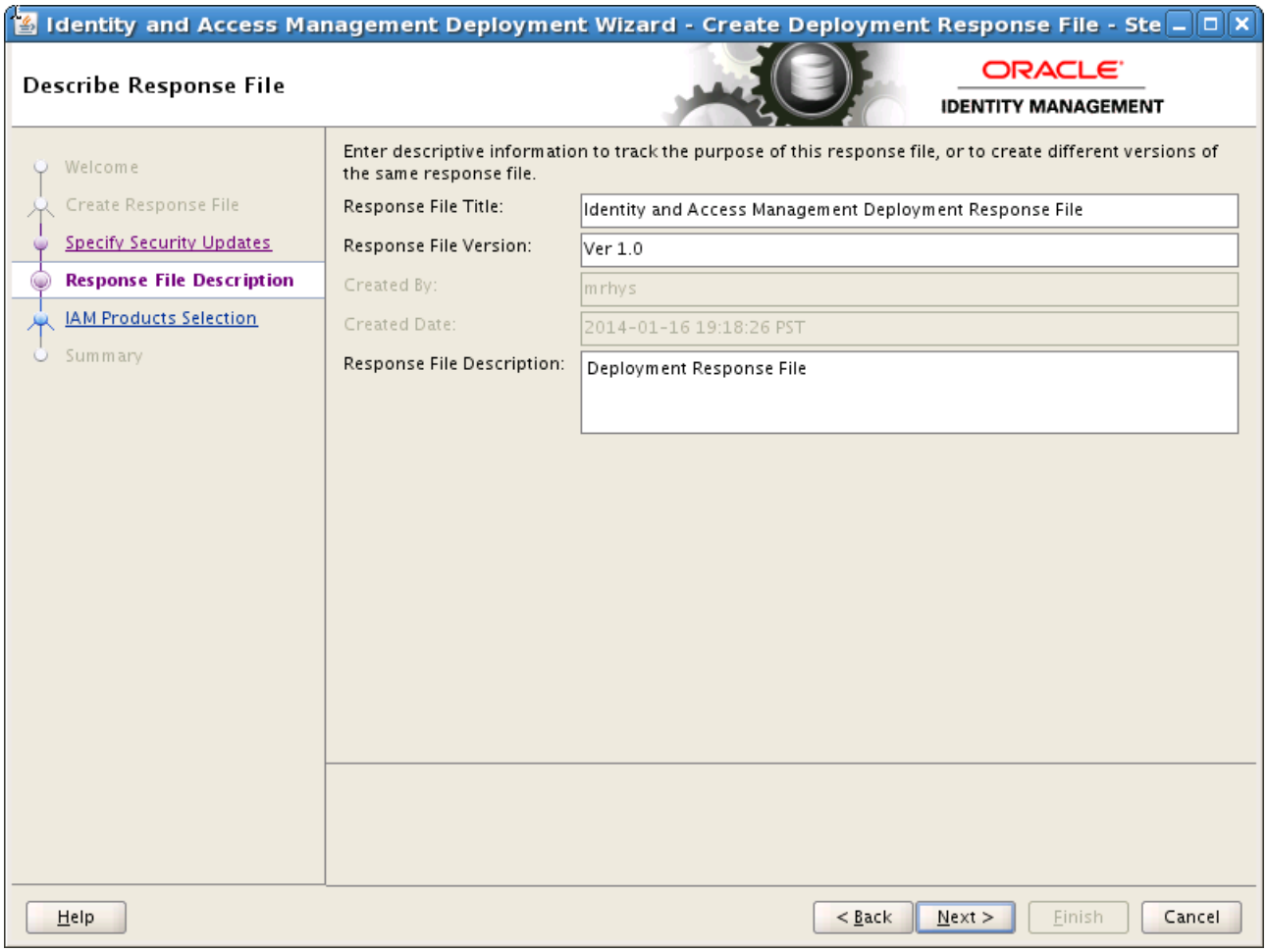


8.4 Describe Response File

On the Describe Response File screen, enter the following information:

- **Response File Title**: A title, such as `Identity and Access Management Deployment Response File`
- **Response File Version**: `Ver 1.0`
- **Response File Description**: A description such as `IAM Deployment Response File`

Click **Next**.

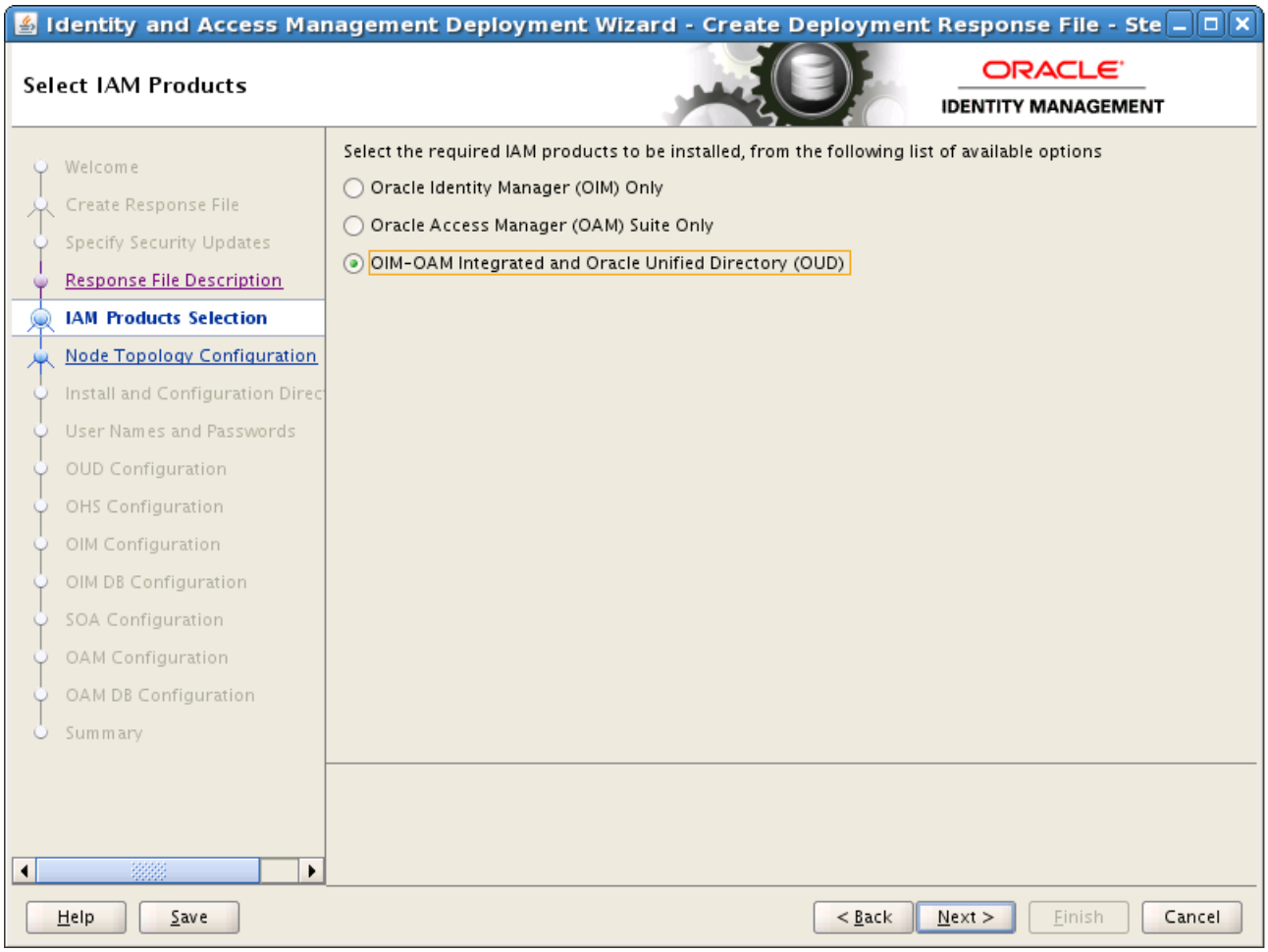


8.5 Select IAM Products

On the Select IAM Products screen select **OIM-OAM Integrated and Oracle Unified Directory (OUD)**.

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

Click **Next**.



8.6 Select Topology

On the Select Topology screen, select **Highly Available (HA)** and provide the following information:

> **Note:** All host names must be fully qualified.

Enter:

- **Directory**: `LDAPHOST1.mycompany.com` (*LDAPHOST1*)
- **Identity Governance /OIM**: `OIMHOST1.mycompany.com` (*OIMHOST1*)
- **Access Management**: `OAMHOST1.mycompany.com` (*OAMHOST1*)
- **Web Tier**: `WEBHOST1.mycompany.com` (*WEBHOST1*)

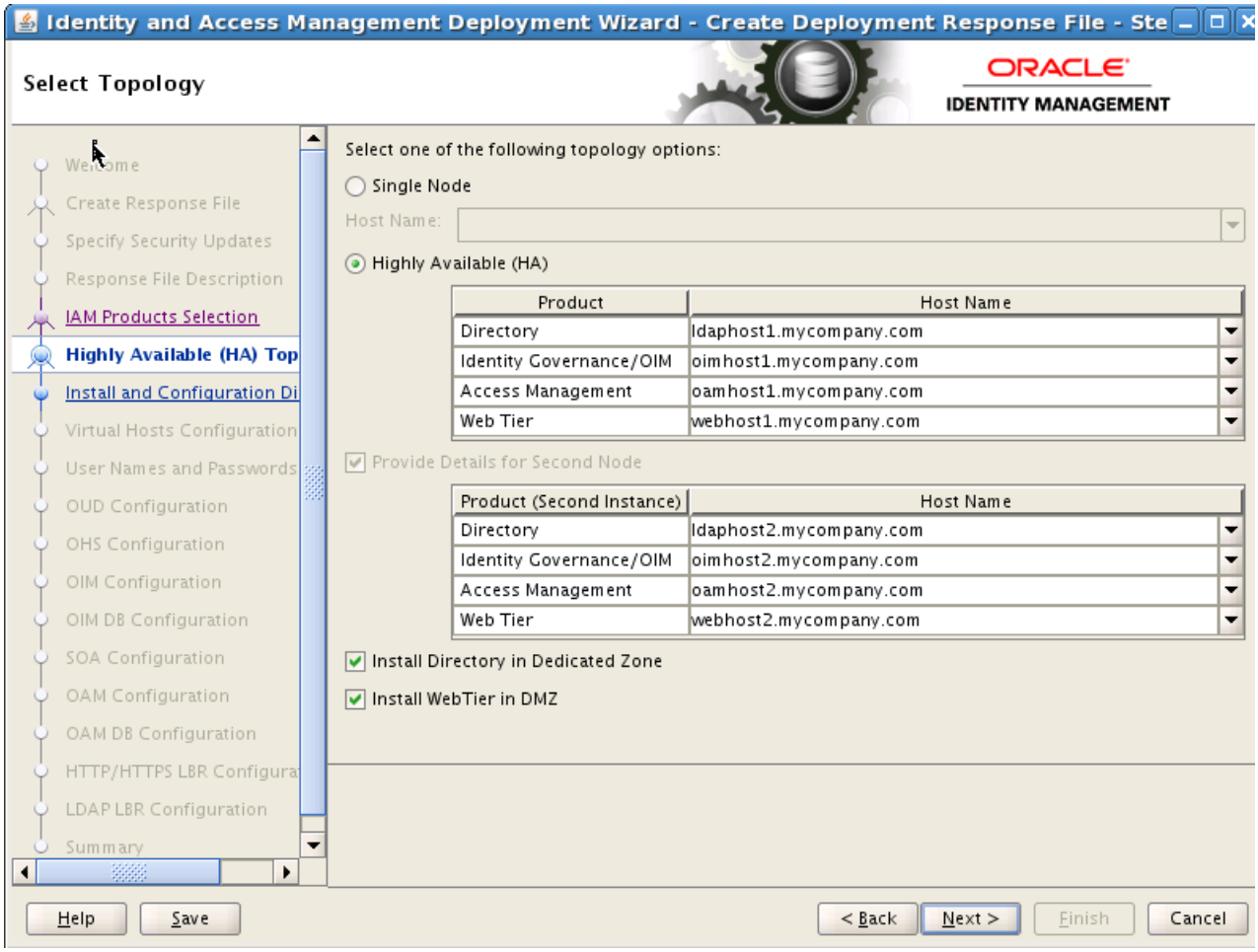
Ensure **Provide Details for Second Node** is selected, then enter the following information.

- **Directory**: `LDAPHOST2.mycompany.com` (*LDAPHOST2*)
- **Identity Governance (OIM)**: `OIMHOST2.mycompany.com` (*OIMHOST2*)
- **Access Management**: `OAMHOST2.mycompany.com` (*OAMHOST2*)
- **Web Tier**: `WEBHOST2.mycompany.com` (*WEBHOST2*)

Select **Install Directory in Dedicated Zone** if your directory servers are in a dedicated security zone and do not share the same *SW_ROOT* directory as the Identity Governance/Access Management Servers. If this option is selected, a separate *SW_ROOT* directory will be shared among the directory servers. See Chapter 4, "Preparing Storage for an Enterprise Deployment" for details.

Select **Install WebTier in DMZ** if you are using a dedicated Web Tier inside a DMZ where the *SW_ROOT* location is local. This is the default Enterprise Deployment Topology.

Note: For Exalogic deployments, **Install WebTier in DMZ** is deselected for all but the Exalogic External OHS topology.



Notes:

- OHS is not placed on the same host as a mid tier or LDAP component. In the topology described in this guide, OHS is located in a DMZ for added security.
- OHS cannot be located on an LDAP host.

Click **Next**.

8.7 Select Installation and Configuration Locations

On the Install Location Configuration Screen, enter the following information:

- **Lifecycle Management Store Location**: This is a location for storing data to support lifecycle management, for example: `/u01/lcm` (*LCM_HOME*)
- If you have mounted your *LCM_HOME* directory on your directory hosts, select **Mounted on Directory hosts**
- If you have mounted your *LCM_HOME* directory on your web hosts then, select **Mounted on Web hosts**

> **Note:** As described in Section 5.7, "Mounting Shared Storage onto the Host," 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 both of these **Mounted on ...** options.
>
> 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 9.4, "Deploying Identity and Access Management Without a Common LCM_HOME" for details.

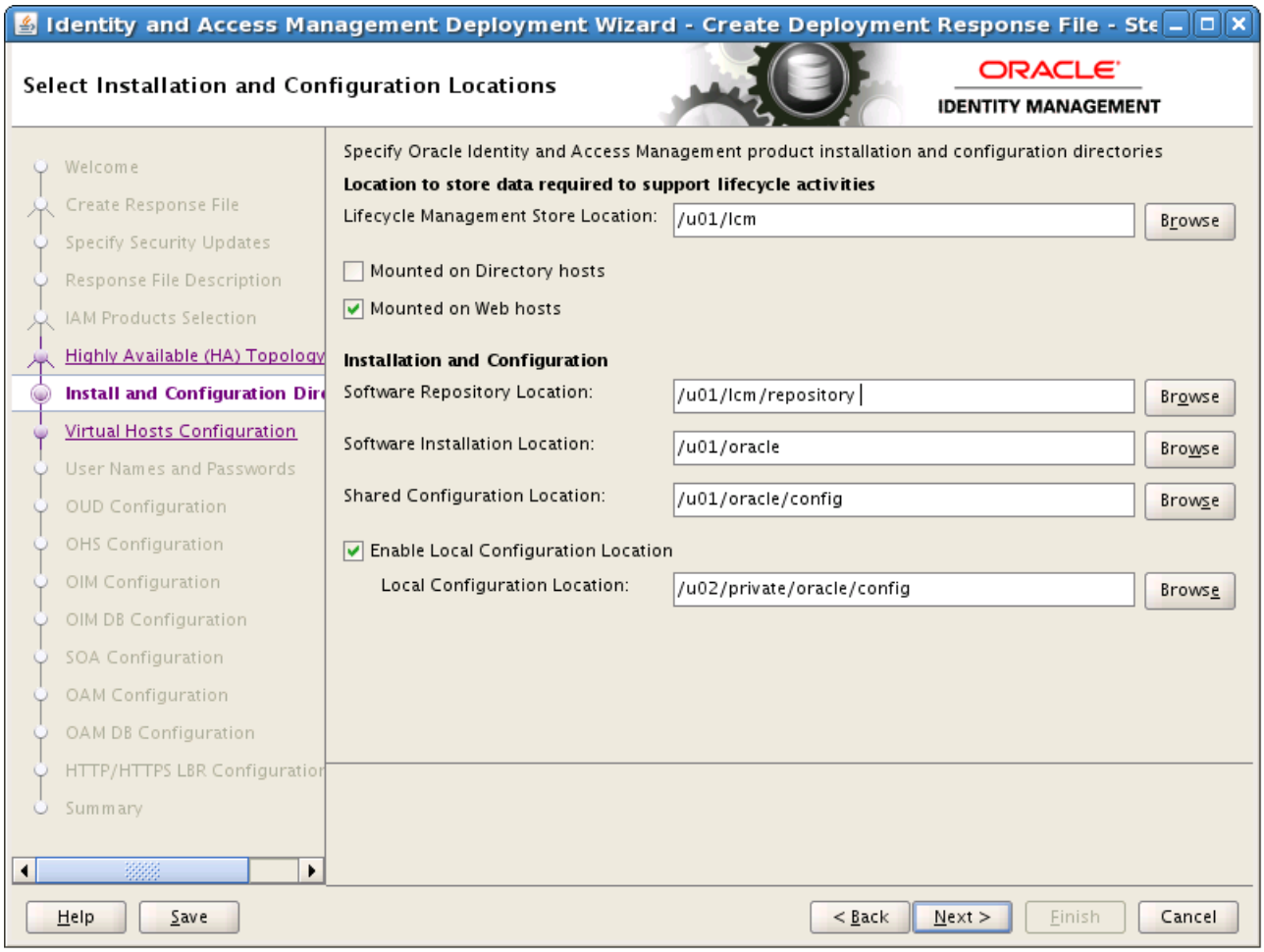
- **Software Repository Location**: This is the location of the Deployment repository, for example: `/u01/lcm/Repository` (*REPOS_HOME* in the worksheet).
- **Software Installation Location**: This is the location on shared storage under where you want the Middleware Home to be placed, for example: `/u01/oracle` (*IDM_TOP*)

> **Note:** Note: The maximum length of this location is 45 characters in this release.

- **Shared Configuration Location**: Enter the location of shared configuration, for example: `/u01/oracle/config` (*SHARED_CONFIG_DIR*).
- **Enable Local Configuration Location**: Select this for Enterprise Deployments.
- **Local Configuration Location**: This is the location on local storage where you want the Oracle HTTP Server Middleware home and local configuration files to be stored, for example: `/u02/private/oracle/config` (*LOCAL_CONFIG_DIR*).

> **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**.

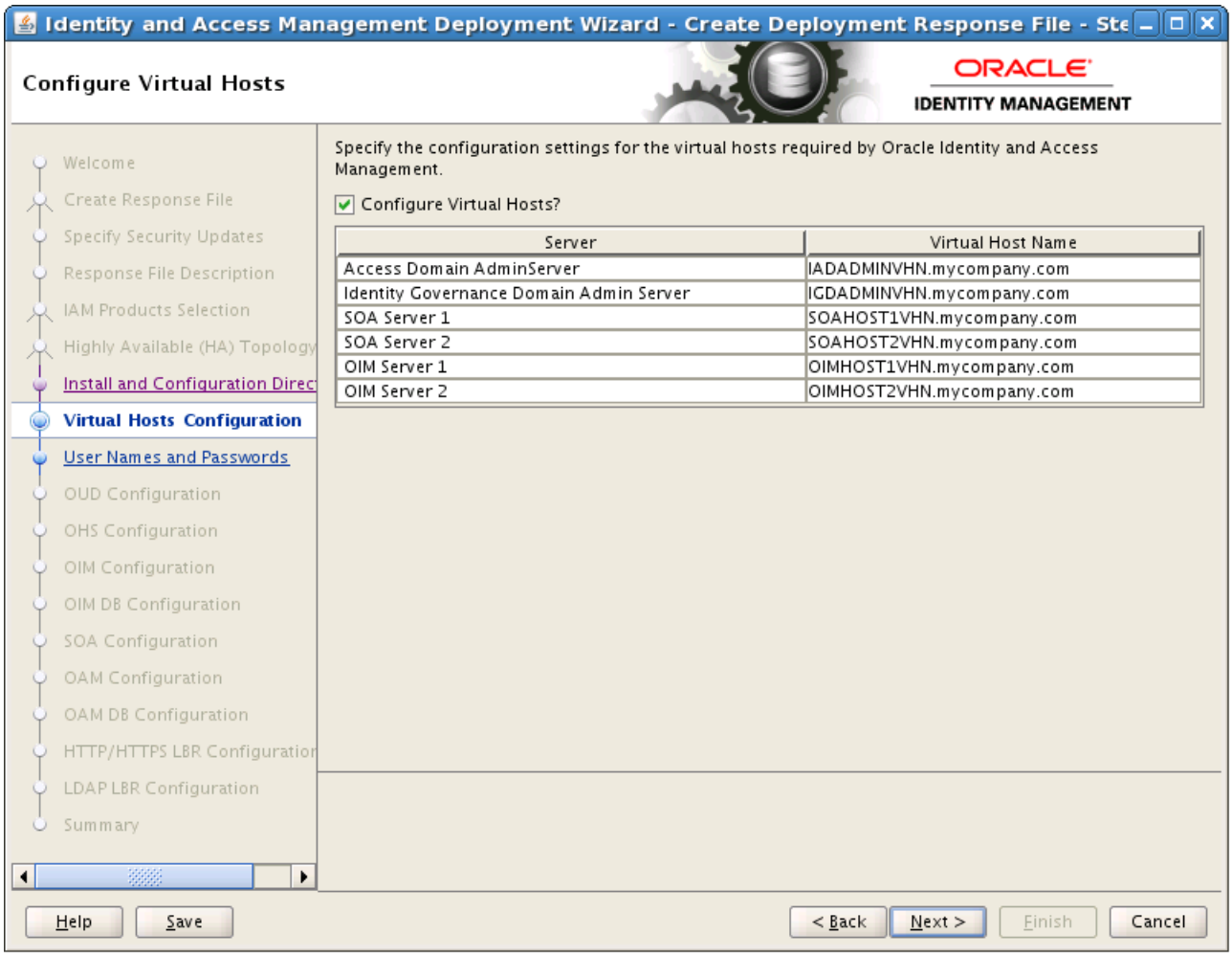


8.8 Configure Virtual Hosts

On the Configure Virtual Hosts screen, select **Configure Virtual Hosts**.

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

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



Click **Next**.

8.9 Set User Names and Passwords

The Usernames 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 (*COMMON_IDM_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.

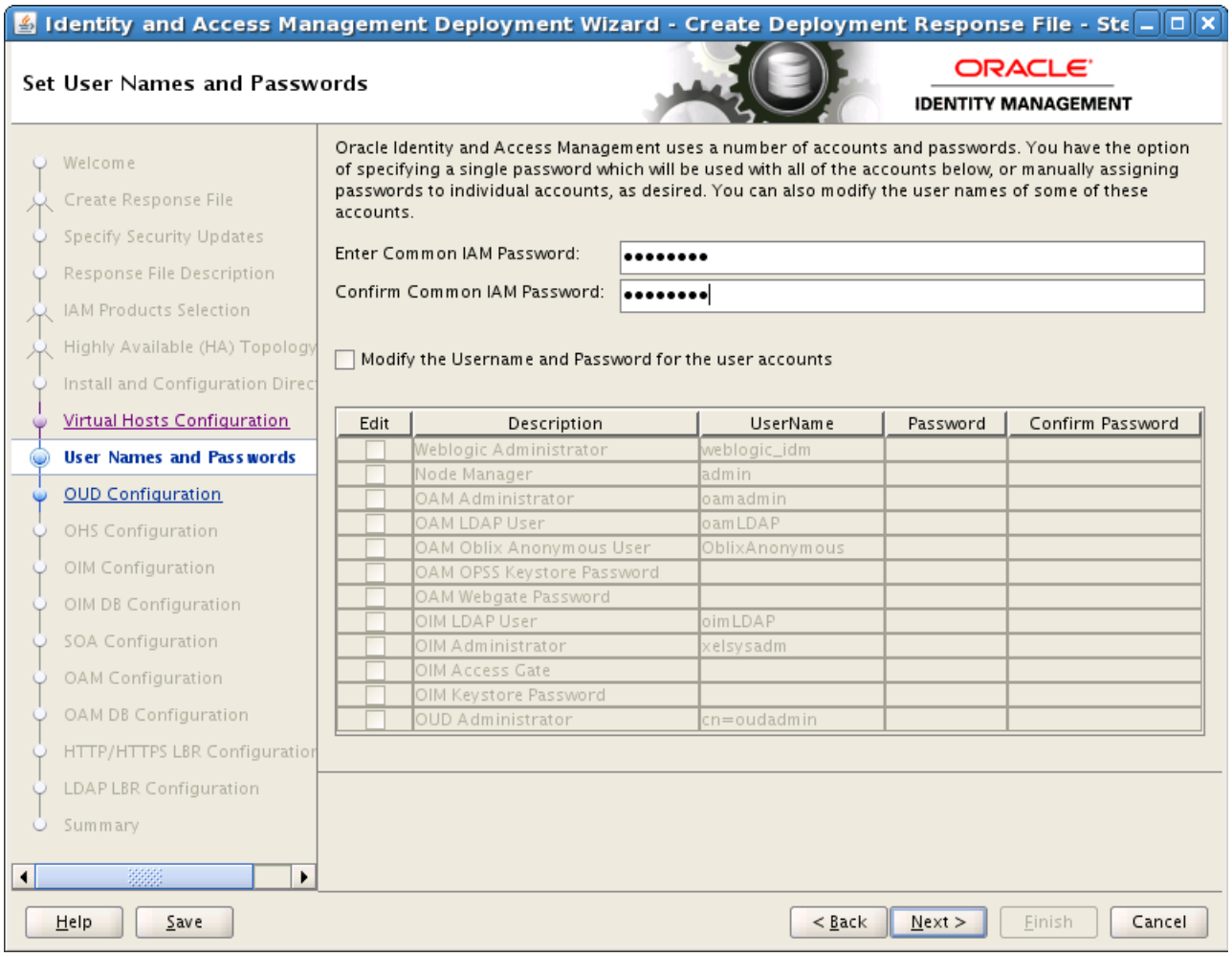
> **Note:** For the purposes of this guide, assume that a Common IAM password is being used.

Modify the Username and Password for the user accounts: Select this if you want to override the default usernames and common password.

Select **Edit** next to the account you wish to modify.

Override the Username and Password as desired.

Click **Next**.



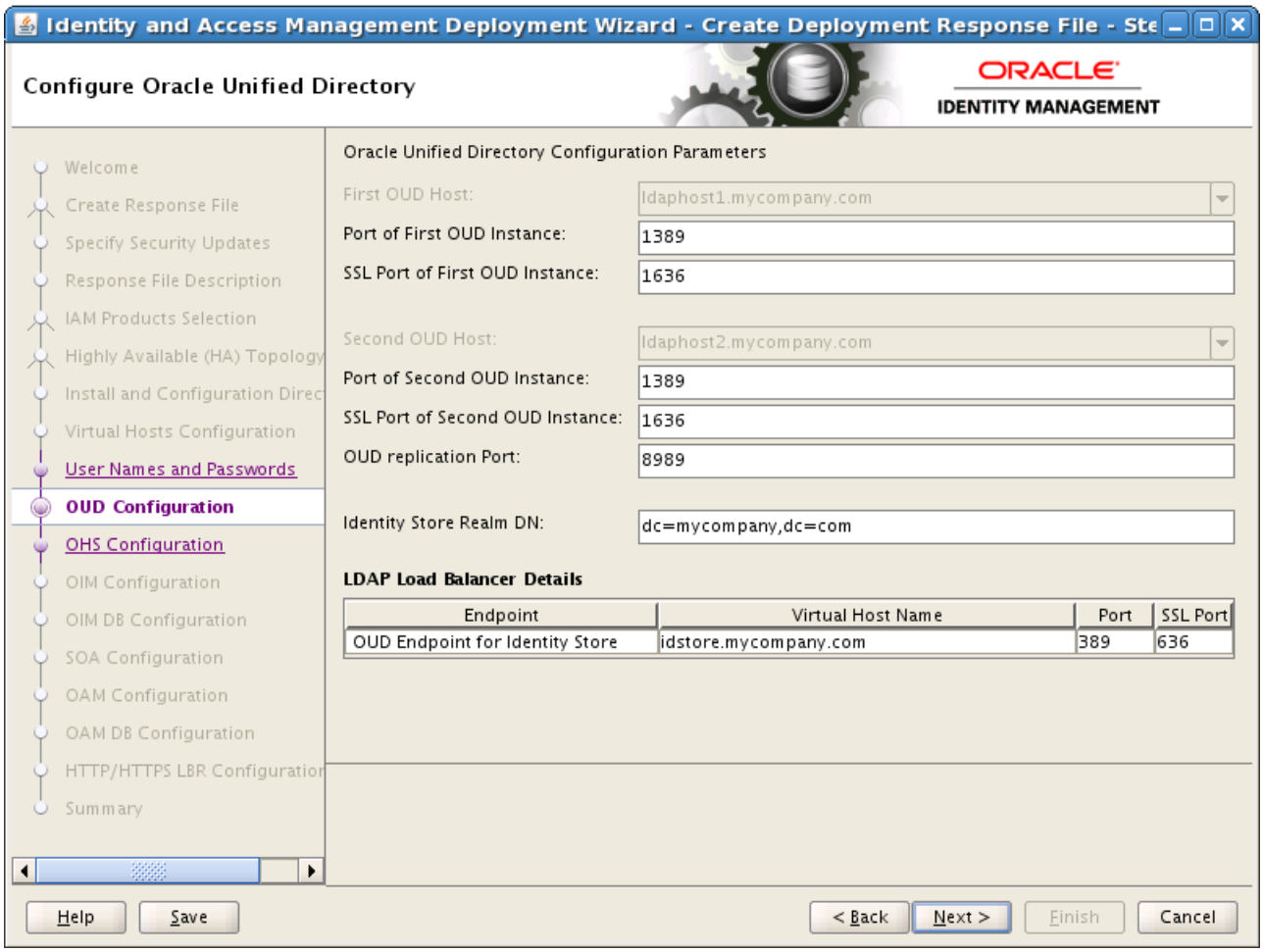
Click **Next**.

8.10 Configure Oracle Unified Directory

On the Oracle Unified Directory Configuration screen, enter the following information:

- **Port of First OUD Instance**: Port to be used for OUD non secure connections on LDAPHOST1, for example: 1389 (*LDAP_PORT*)
- **SSL Port of First OUD Instance**: Port to be used for OUD secure connections on LDAPHOST1, for example: 1636 (*LDAP_SSL_PORT*)
- **Port of Second OUD Instance**: Port to be used for OUD non secure connections on LDAPHOST2, for example: 1389 (*LDAP_PORT*)
- **SSL Port of Second OUD Instance**: Port to be used for OUD secure connections on LDAPHOST2, for example: 1636 (*LDAP_SSL_PORT*)
- **OUD Replication Port**: 8989 (*LDAP_REPLIC_PORT*)
- **Identity Store Realm DN**: `dc=mycompany,dc=com` (*REALM_DN*)
- **LDAP Load Balancer Details**:

- **Endpoint**: The name of the endpoint, for example: `OUD Endpoint for ID Store`
- **Virtual Host Name**: The virtual host of the Identity store, for example: idstore.mycompany.com (*LDAP_IDSTORE_NAME*)
- **Port**: 1389 (*LDAP_LBR_PORT*)
- **SSL Port**: 1636 (*LDAP_LBR_SSL_PORT*)



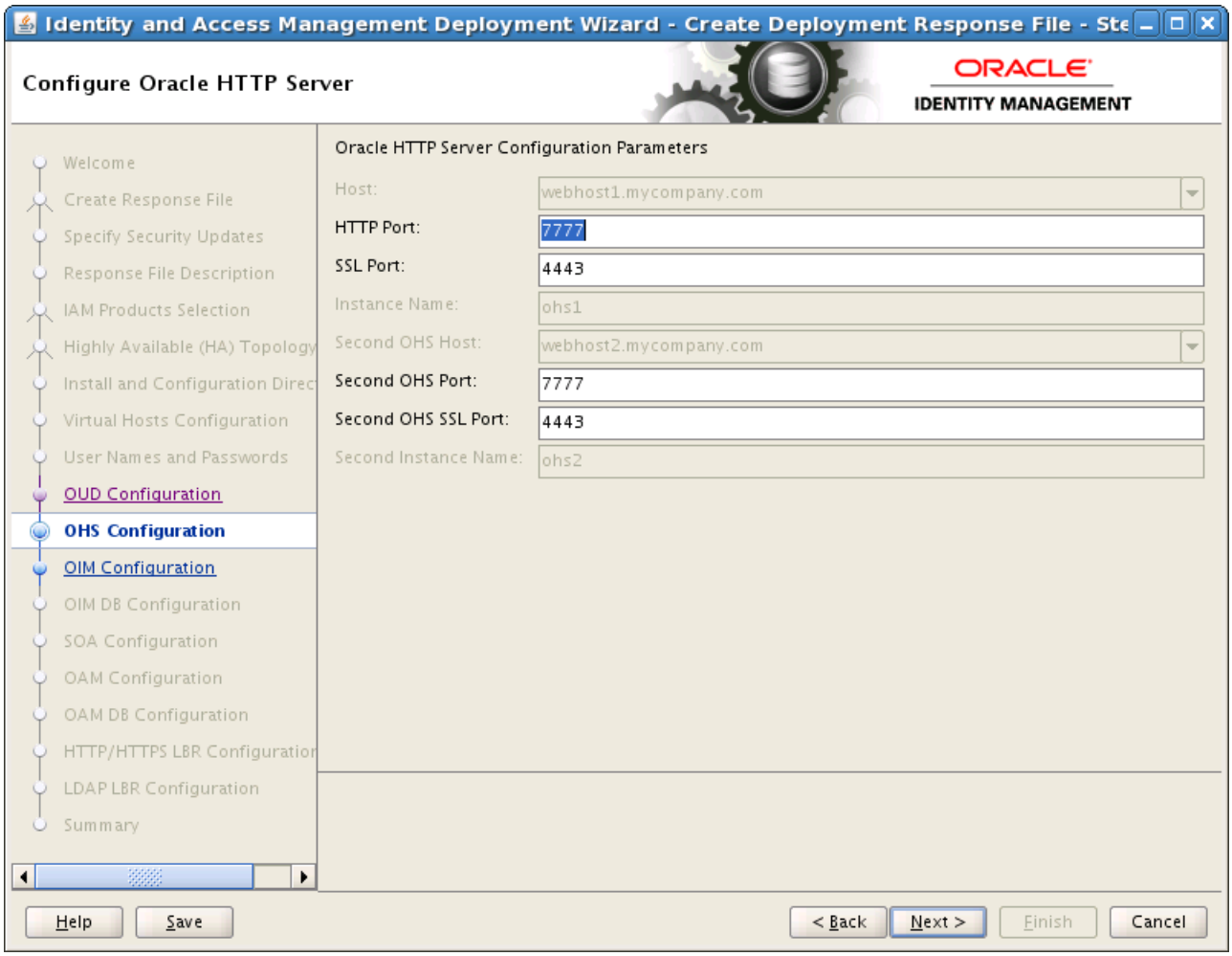
Click **Next**.

8.11 Configure Oracle HTTP Server

On the Oracle HTTP Server Configuration screen, if necessary, change the port numbers to the ports that the Oracle HTTP Server managed servers will use. For example:

- **Port**: 7777 (*WEB_HTTP_PORT*)
- **SSL Port**: 4443 (*WEB_HTTPS_PORT*)
- **Second OHS Port**: 7777 (*WEB_HTTP_PORT*)
- **Second OHS SSL Port**: 4443 (*WEB_HTTPS_PORT*)

Click **Next**.



8.12 Configure Oracle Identity Manager

On the Oracle Identity Manager Configuration screen, under **Oracle Identity Manager Configuration Parameters**, enter the following information:

Admin Server Port: The port number that the IAMGovernanceDomain Administration Server will use, for example: 7101 (*IGD_WLS_PORT*)

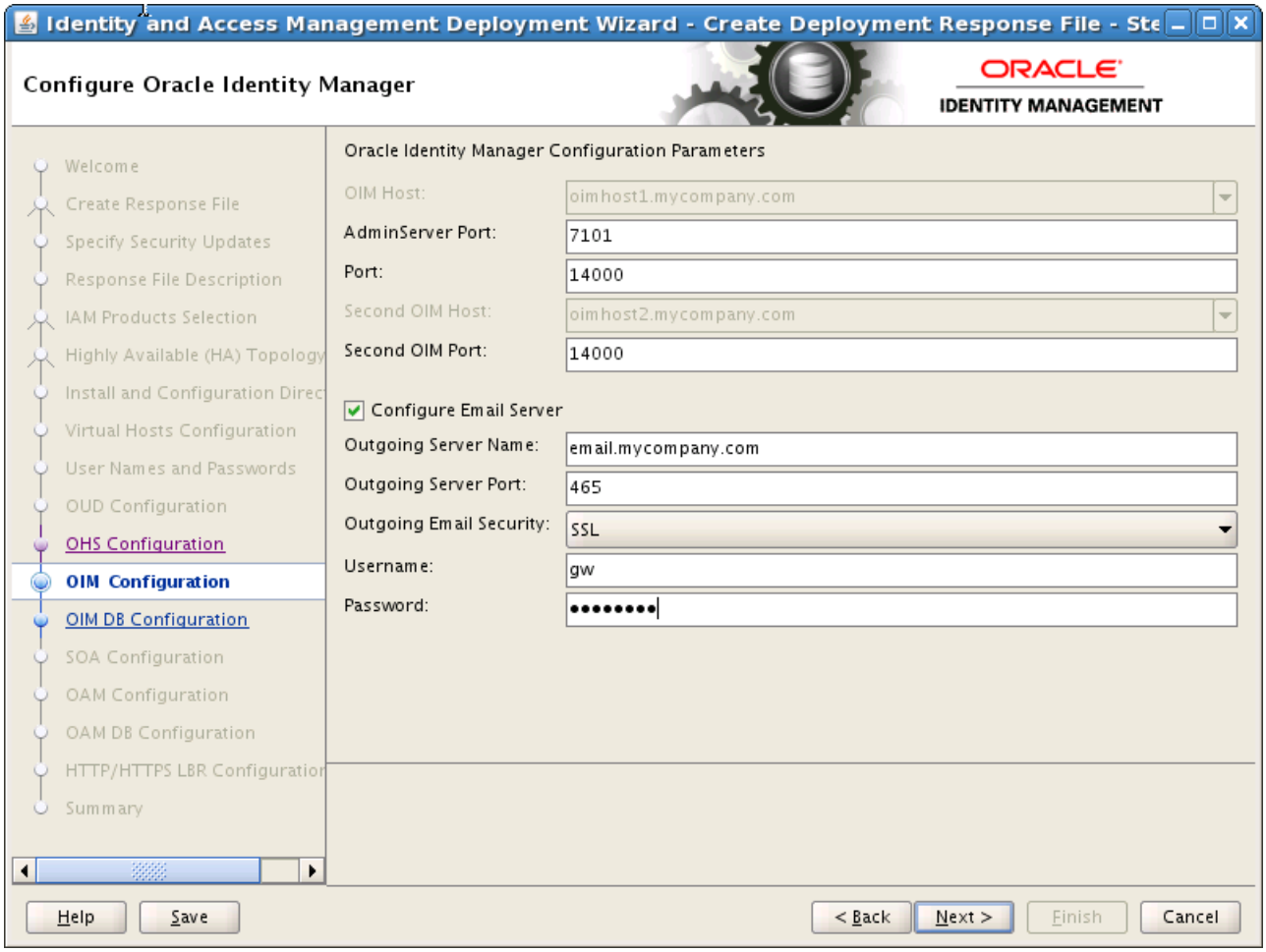
Port: The port number that the first OIM Managed Server will use, for example: 14000 (*OIM_PORT*)

Second OIM Port: The port number that the second Managed Server will use, for example: 14000 (*OIM_PORT*)

If you want to configure OIM to send Email Notifications, select **Configure Email Server** and provide the following details:

- **Outgoing Server Name**: The name of your outgoing email server, for example: `EMAIL.mycompany.com` (*EMAIL_SERVER*)
- **Outgoing Server Port**: The port your email server uses, for example: 465 (*EMAIL_PORT*).
- **Outgoing Email Security**: Select `None`, `SSL`, or `TLS` (*EMAIL_PROTOCOL*)

- **Username**: The username (*EMAIL_USER*) you use to authenticate with the email server.
- **Password**: Password (*EMAIL_PASSWORD*) for the above user.



Click **Next**.

8.13 Configure Oracle Identity Manager Database

On the Oracle Identity Manager DB Configuration screen, enter the details about the Oracle Database where Identity Manager information will be stored.

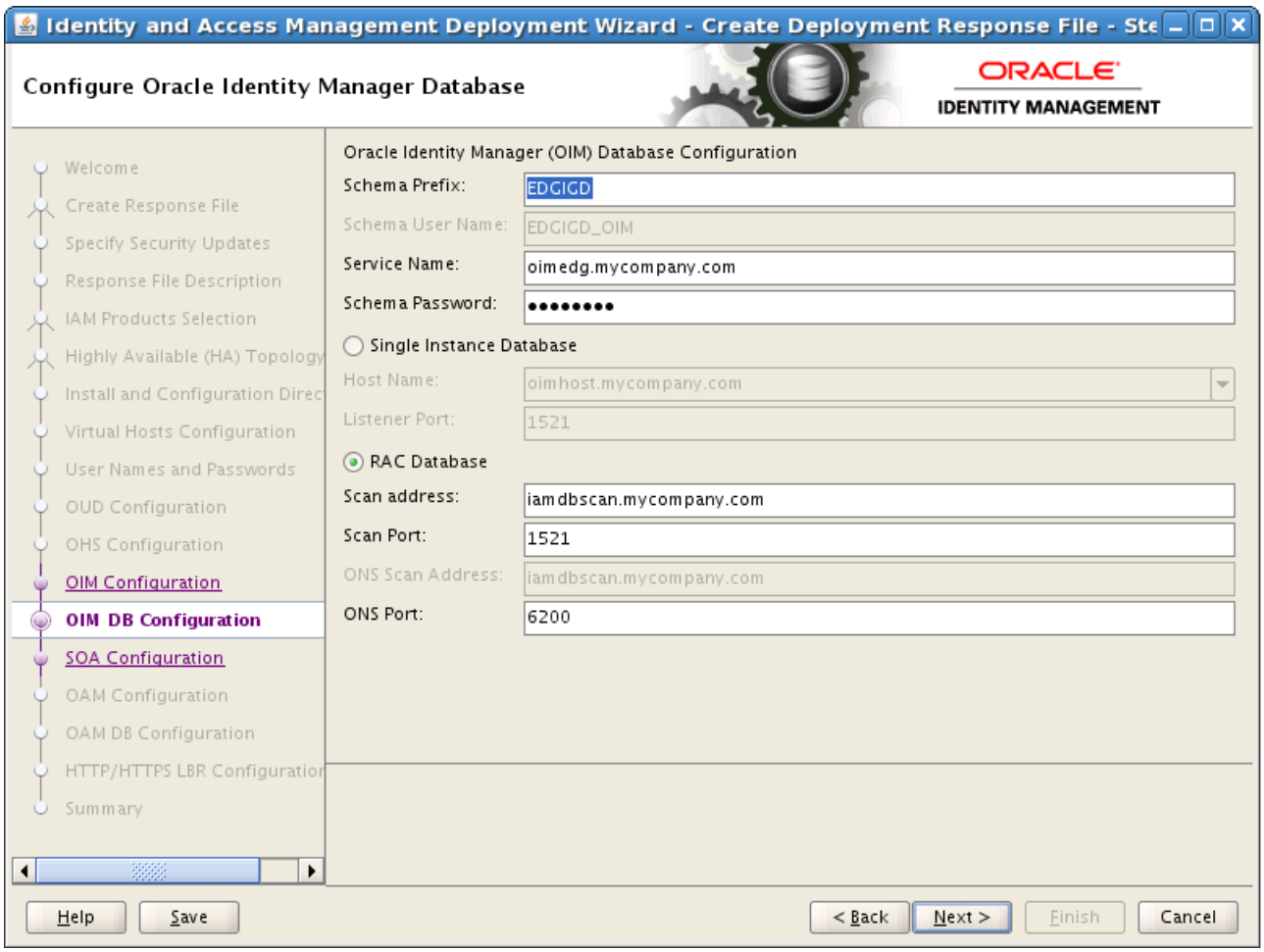
- **Schema Prefix**: This is the Prefix that was used when the Repository Creation assistant was run to create the Database Schemas. For example: EDGIGD.
- **Service Name**: The service name of the database service, for example `OIMEDG.mycompany.com` (*OIM_DB_SERVICENAME*)
- **Schema Password**: The password you used when creating the Oracle Identity Manager schema in RCU, *OIM_SCHEMA_PASSWORD*.
- Select **RAC DB**.
- **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com` (*SCAN_ADDRESS*)

Note: The default value for the Oracle Notification Server (ONS) Scan Address, used by Gridlink, is the Database scan address.

- **Scan Listener Port**: Enter the port used by the Grid Infrastructure Listener, for example: 1521 (*DB_LSNR_PORT*)
- **Scan port**: Determine the Scan (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**.

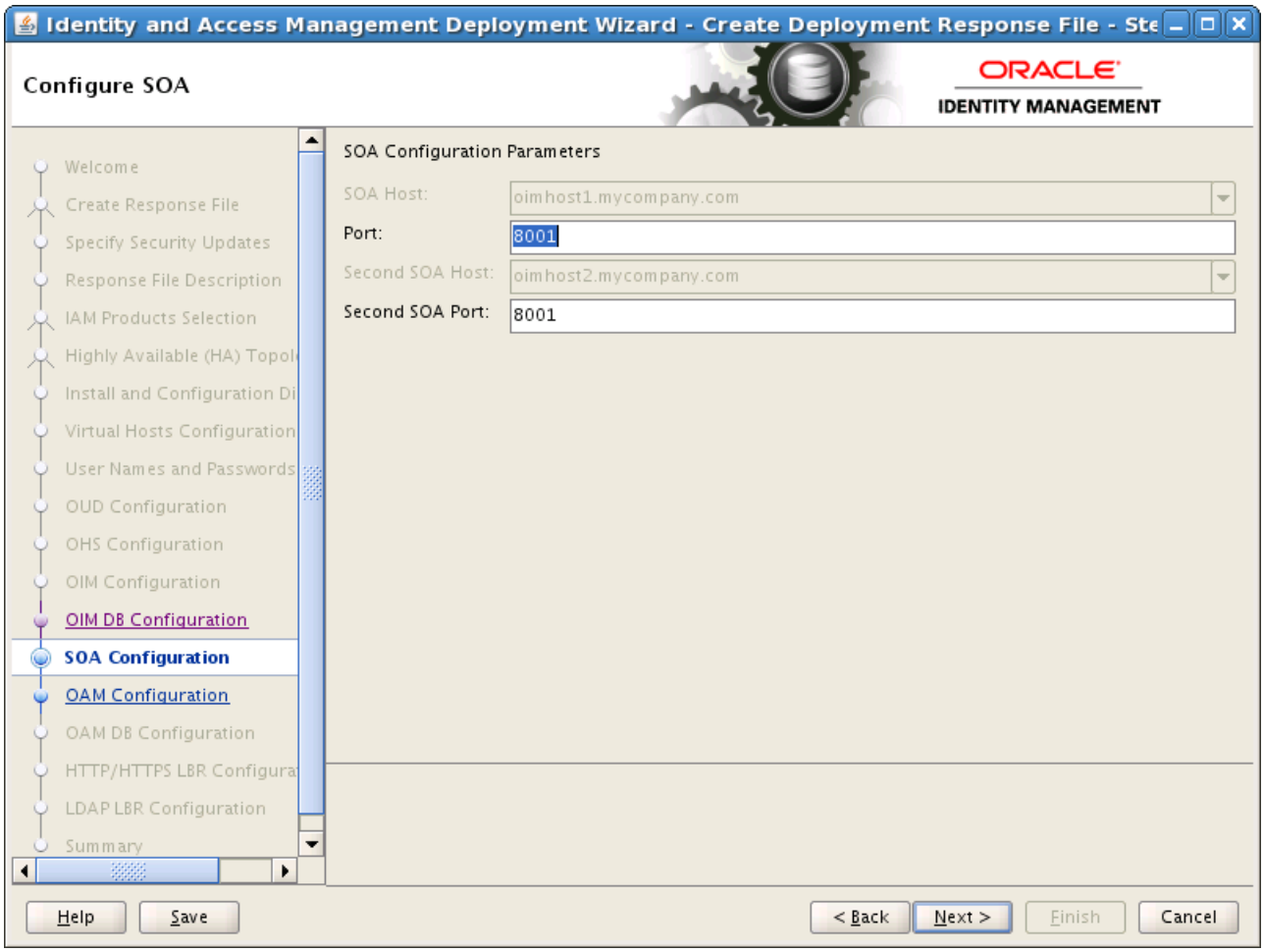


8.14 Configure SOA

Enter the following information:

- **Port**: The Port that the first SOA Managed server will use, for example: 8001 (*SOA_PORT*)
- **Second SOA Port**: The Port that the second SOA Managed server will use, for example: 8001 (*SOA_PORT*)

Click **Next**

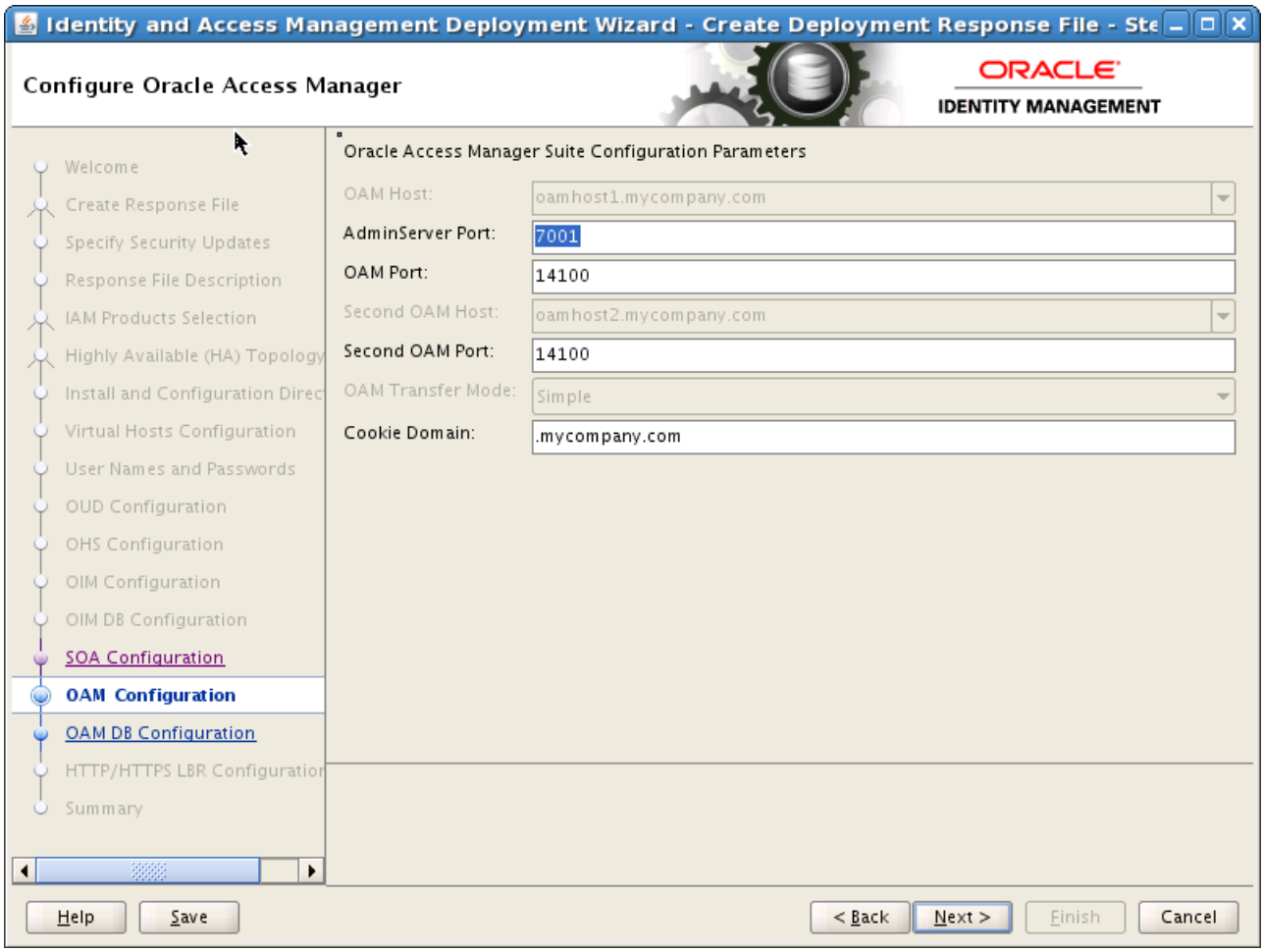


8.15 Configure Oracle Access Manager

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

- **Admin Server Port**: The Port that the IAMAccessDomain Administration Server will use, for example: 7001 (*IAD_WLS_PORT*)
- **OAM Port**: The Port that the first OAM Managed Server will use, for example: 14100 (*OAM_PORT*)
- **Second OAM Port**: The Port that the second OAM Managed Server will use, for example: 14100 (*OAM_PORT*)
- **Cookie Domain**: for example: `.mycompany.com` (*OAM_COOKIE_DOMAIN*)

Click **Next**.



8.16 Configure Oracle Access Manager Database

By default, the Oracle Access Manager DB Configuration screen shows the same values as the Configure Oracle Identity Manager screen. If necessary, enter the details about the Oracle Database where Access Manager information will be stored.

- **Schema Prefix**: This is the Prefix that was used when the Repository Creation assistant was run to create the Database Schemas. For example: EDGIAD.
- **Service Name**: The service name of the database service, for example `OAMEDG.mycompany.com` (*OAM_DB_SERVICENAME*)
- **Schema Password**: The password you used when creating the Oracle Access Manager schema in RCU, *OAM_SCHEMA_PASSWORD*.
- Select **RAC DB**.
- **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com` (*SCAN_ADDRESS*)

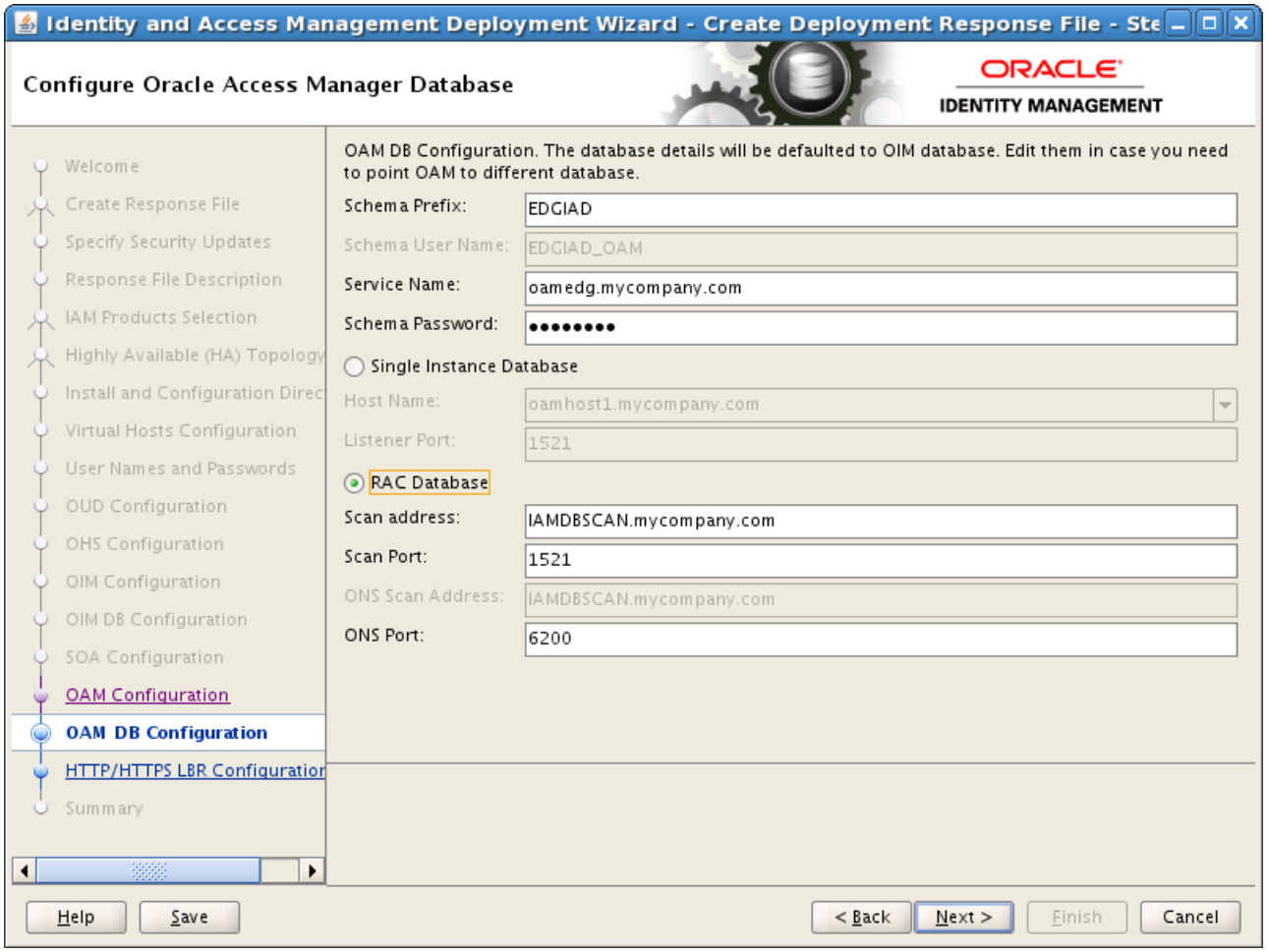
> **Note:** The default value for the Oracle Notification Server ONS) Scan Address, used by Gridlink, is the Database scan address.

- **Scan Listener Port**: Enter the port used by the Grid Infrastructure Listener, for example: 1521 (*DB_LSNR_PORT*)

- **Scan port**: Determine the Scan (ONS) port by using the `srvctl` command, as shown in the following example:

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

Click **Next**.



Click **Next**

8.17 Configure HTTP/HTTPS Load Balancer

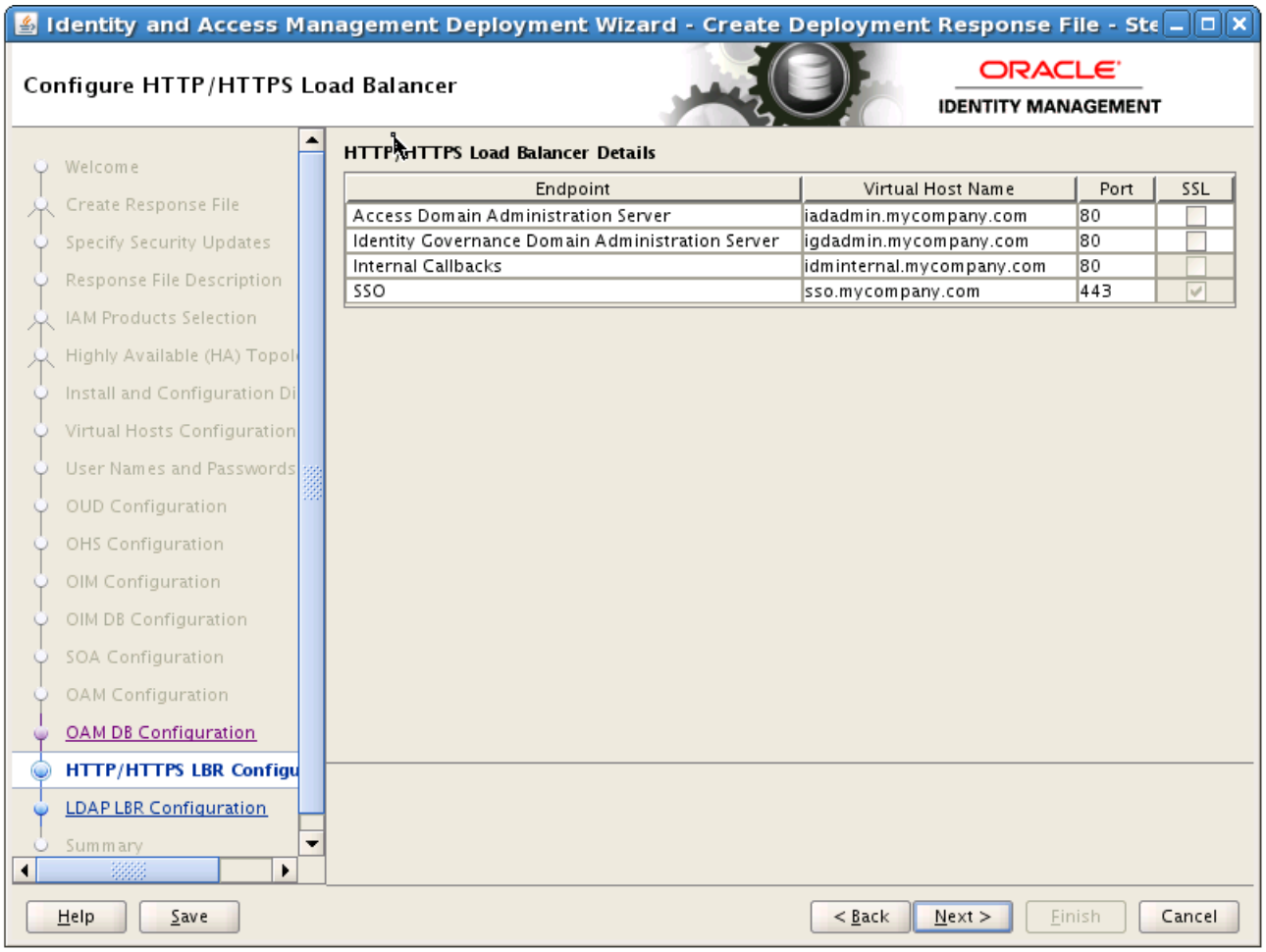
On the HTTP/HTTPS Load Balancer screen, enter details about your load balancer virtual hosts.

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

- **IAM Access Domain Admin**: The Load Balancer end point used to access the IAMAccessDomain Administration functions, (*IAD_DOMAIN_LBRVHN*) for example: `IADADMIN.mycompany.com` Port `80`, Not SSL
- **IAM Governance Domain Admin**: The Load Balancer end point used to access the IAMGovernanceDomain Administration functions (*IGD_DOMAIN_LBRVHN*), for example: `IGDADMIN.mycompany.com` Port `80`, not SSL

- **Internal Callbacks**: This is the internal call back virtual host and port (*IAM_INTERNAL_LBRVHN*), for example: idminternal.mycompany.com, Port 80
- **SSO**: This is the main application entry point (*IAM_LOGIN_LBRVHN*), for example: sso.mycompany.com Port 443, always SSL.

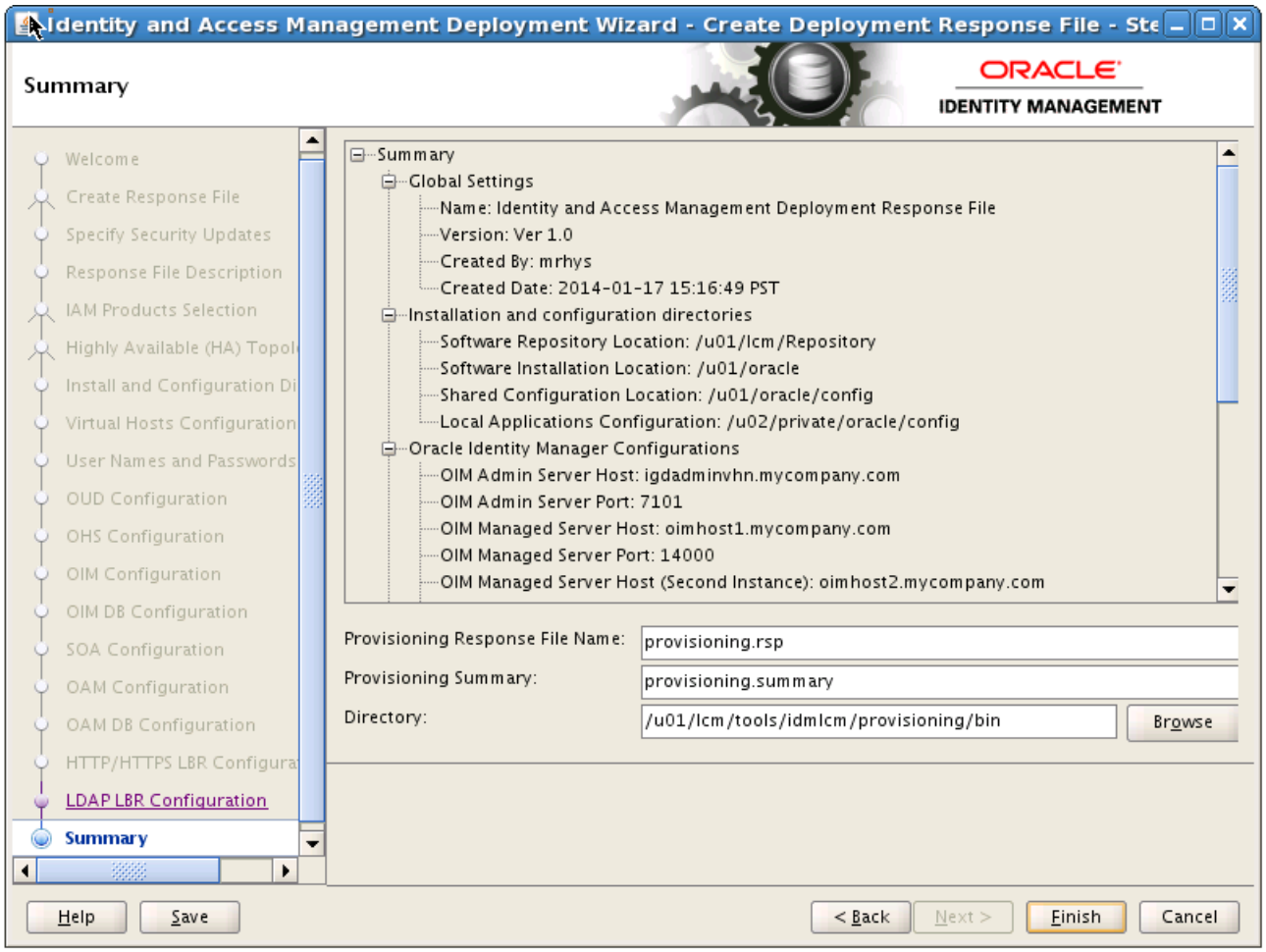
Note: The four virtual host names entered on this screen must be unique.



8.18 Summary

On the Summary screen, enter the **Deployment Response File Name** and the **Directory** where it is to be stored. You can change the **Deployment Summary** field or leave it at the default value.

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."



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

9

Deploying Identity and Access Management

This chapter describes how to deploy Identity and Access Management.

It contains the following sections:

9.1 Introduction to the Deployment Process

This section introduces the Deployment process.

9.1.1 Deployment Stages

There are eight stages to Deployment. These stages are:

1. preverify - This checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured. This also checks for database connections for schemas and port availability,
2. install - This installs all of the software required by the installation. This also includes binary patching for all of the patches included in the repository.
3. preconfigure - This does the following:
   - Creates Oracle Unified Directory instances and seeds them with Users/Groups.
   - Creates the WebLogic domains and extends domains for various products
   - Creates OHS instance
   - Migrates the Policy Store to the database
4. configure - This does the following:
   - Starts managed servers as necessary
   - Associates Access Manager with Oracle Unified Directory
   - Configure Oracle Identity Manager
5. configure-secondary - This does the following:
   - Integrates Weblogic Domain with Webtier

- Register webtier with domain
- Integrate Access Manager and Oracle Identity Manager

6. postconfigure - This does the following:
   - Run Oracle Identity Manager Reconciliation
   - Configure UMS Mail Server
   - Generate Access Manager Keystore
   - Configure WebGates
7. startup - This starts up all components in the topology and applies any needed artifact patches.
8. validate - This performs a number of checks on the built topology to ensure that everything is working as it should be.

Each stage must be completed on all hosts in a specific order, as described in the next section. Each stage must be completed on each host in the topology before the next stage can begin. Failure of a stage will necessitate a cleanup and restart. See Appendix B, "Cleaning Up an Environment Before Rerunning IAM Deployment" for instructions.

9.1.2 Processing Order

You must process hosts in the following order:

1. LDAP Host 1
2. LDAP Host 2
3. Identity Governance Host 1
4. Identity Governance Host 2
5. Access Management Host 1
6. Access Management Host 2
7. Web Host 1
8. Web Host 2

This equates to the following order for hosts in this guide.

Consolidated List

1. IAMHOST1
2. IAMHOST2
3. WEBHOST1
4. WEBHOST2

Distributed List

1. LDAPHOST1
2. LDAPHOST2
3. OIMHOST1
4. OIMHOST2
5. OAMHOST1

6. OAMHOST2
7. WEBHOST1
8. WEBHOST2

9.2 Deployment Procedure

The following sections describe the procedure for performing Deployment.

- Section 9.2.1, "Running the Deployment Commands"
- Section 9.2.2, "Creating Backups"

9.2.1 Running the Deployment Commands

To deploy Identity and Access Management, run the `runIAMDeployment.sh` a number of times on each host in the topology from the following location:

`IDMLCM_HOME/provisioning/bin`

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

Notes:

- You must use the SAME version of the Deployment profile (*IDMLCM_HOME*`/provisioning/bin/provisioning.rsp`) on all targets and all hosts in the deployment.
- You MUST run each command on each host in the topology, in the specified order, 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
```

9.2.2 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.

9.3 Check List

To help keep track of the Deployment process, print this check list from the PDF version of this guide. Run each stage on the hosts shown, and add a check mark to the corresponding row when that run is complete.

Consolidated:

Deployment Stage	Host	Complete
Preverify	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Install	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Preconfigure	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Configure	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Configure Secondary	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Post Configure	IAMHOST1	

Deployment Stage	Host	Complete
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Startup	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Validate	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	

Distributed:

Deployment Stage	Host	Complete
Preverify	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Install	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Preconfigure	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	

Deployment Stage	Host	Complete
	WEBHOST2	
Configure	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Configure Secondary	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Post Configure	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Startup	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Validate	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	

Deployment Stage	Host	Complete
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	

9.4 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 8.18, "Summary" to the same location on each of the hosts.
3. The deployment tool relies on the contents of the directories located under LCM_HOME/provisioning to determine what stages have run successfully. Therefore, after every command, copy the contents of this directory to every node before executing any runIAMDeployment.sh commands.

   If *LCM_HOME* is not shared to the directory hosts, copy *LCM_HOME*/internal from OAMHOST1 to LDAPHOST1 and LDAPHOST2 before running preconfigure on the LDAPHOSTs.

   LCM_HOME/internal is created after the install phase on the OAMHOSTs.
4. Before running preconfigure on OIMHOST1, copy *LCM_HOME*/keystores from LDAPHOST1 to OAMHOST1.
5. 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-secondary phase on OAMHOST1.

10

Performing Post-Deployment Configuration

This chapter describes tasks you must perform after Deployment.

It contains the following sections:

10.1 Post-Deployment Steps for OPSS

In this release of Identity and Access Management, an optimized OPSS is available. In order to use this optimized OPSS, you must upgrade the OPSS schema. The deployment tool does not do this, so you must perform this step manually, by using Patch Set Assistant, at the end of provisioning.

To upgrade the OPSS schema for EDGIAD and EDGIGD:

1. Start the patch set assistant by running the command psa from the location *IAD_MW_HOME*/oracle_common/bin, for example:

   ```
   ./psa
   ```

2. On the Welcome Screen click **Next**.
3. On the Select Component Screen select **Oracle Platform Security Services** ONLY and click **Next**.
4. On the Prerequisites screen, specify whether or not you have a database backup and that the database version is certified.

   Click **Next**.
5. On the Schema Page, Enter:
   - **Schema User Name**: For example: EDGIAD_OPSS
   - **Password**: Password supplied when RCU was run.
   - **Database** Type: Oracle Database
   - **Connect String**: IDMDB-SCAN*OAM*:*DB_LSNR_PORT*/*OAM_DB_SERVICENAME* for example: IAMDB-SCAN.mycompany.com:1521/oamedg.mycompany.com

- **DBA User Name**: `sys as sysdba`
- **DBA Password**: *PASSWORD*

Click **Connect**.

Click **Next**.

6. On the Examine Page, verify that **Successful** is displayed and click **Next**.
7. On the Upgrade Summary Page verify that the information is correct and click **Upgrade**.
8. Once the upgrade is finished, click **Next**.
9. On the Upgrade Success page, click **Close**
10. Verify that the schema upgrade has been successful by checking the log files located in

    IAD_MW_HOME/oracle_common/upgrade/logs/psa/psatimestamp.log

11. Restart the domain.
12. After upgrading the OPSS schema, run the following command:

    ```
    SELECT VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY WHERE
    OWNER='<RCU_Prefix>_OPSS';
    ```

    The version should now be 11.1.1.7.2 and the **Upgrade** flag is `Yes`.

10.2 Post-Deployment Steps for Oracle Unified Directory

Perform the following steps for Oracle Unified Directory.

10.2.1 Update Oracle Unified Directory Change Log Access

If you are using Oracle Unified Directory and Oracle Identity Manager, grant access to the change log by performing the following steps on all OUD hosts (LDAPHOST1 and LDAPHOST2).

To grant access to the change log:

1. Remove the existing change log permission by issuing this command on one of the replicated OUD hosts:

    ```
    OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
    --remove
    global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
    acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)" \
            --hostname OUD_HOST \
            --port OUD_ADMIN_PORT \
            --trustAll \
            --bindDN cn=oudadmin \
            --bindPasswordFile passwordfile \
            --no-prompt
    ```

    For example:

    ```
    OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
    --remove
    global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
    acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)" \
            --hostname LDAPHOST1.mycompany.com \
    ```

```
        --port 4444 \
        --trustAll  \
        --bindDN cn=oudadmin \
        --bindPasswordFile mypasswordfile \
        --no-prompt
```

2. Then add the following new ACI:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname OUD_HOST \
        --port OUD_ADMIN_PORT \
        --trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
        --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname LDAPHOST1.mycompany.com \
        --port 4444 \
        --trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile mypasswordfile \
        --no-prompt
```

10.2.2 Update Oracle Unified Directory ACIs for LDAP Synchronization

The following is a workaround for an Oracle Unified Directory operations failure when LDAP synchronization is enabled

In an environment in which LDAP synchronization is enabled, certain operations against Oracle Unified Directory fail with the following error in Oracle Unified Directory logs:

```
The request control with Object Identifier (OID) "1.2.840.113556.1.4.319" cannot
be used due to insufficient access rights
```

To work around this issue, you must edit a configuration file on both instances of Oracle Unified Directory.

1. Change the ACIs on control 1.2.840.113556.1.4.319 from `ldap://all` to `ldap://anyone` in the Oracle Unified Directory config file *OUD_ORACLE_INSTANCE*`/OUD/config/config.ldif`, as shown:

   Change:

```
ds-cfg-global-aci: (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 ||
1.3.6.1.1.13.2 || 1.2.840.113556.1.4.319 || 1.2.826.0.1.3344810.2.3 ||
2.16.840.1.113730.3.4.18 || 2.16.840.1.113730.3.4.9 || 1.2.840.113556.1.4.473
|| 1.3.6.1.4.1.42.2.27.9.5.9") (version 3.0; acl "Authenticated users control
access"; allow(read) userdn="ldap:///all";)
```

To:

```
ds-cfg-global-aci: (targetcontrol="2.16.840.1.113730.3.4.2 ||
2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 || 1.3.6.1.4.1.4203.1.10.2
|| 1.3.6.1.4.1.42.2.27.8.5.1 || 2.16.840.1.113730.3.4.16 ||
2.16.840.1.113894.1.8.31 || 1.2.840.113556.1.4.319") (version 3.0; acl
"Anonymous control access"; allow(read) userdn="ldap:///anyone";)
```

2. Restart the Oracle Unified Directory server as described in Section 15.1, "Starting and Stopping Components."

10.3 Post-Deployment Steps for Oracle Identity Manager

Perform the following post-deployment steps.

- Section 10.3.1, "Post Deployment Steps to Address Known Issue"
- Section 10.3.2, "Update Server Start Parameters"

10.3.1 Post Deployment Steps to Address Known Issue

Due to a known issue, node manager SSL is not configured fully. The workaround is to perform the following steps for each administration and managed server in the deployment, in each domain.

1. Login to the WebLogic console for the domain using at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **Lock and Edit**.
3. Navigate to **Environment > Servers**
4. Click on a server name, for example: **wls_oam1**
5. Click on the **SSL** tab
6. Expand the **Advanced Options** and change **Hostname Verification** to **BEA Host Name Verifier**
7. Click **Save**.
8. Repeat for each server in the domain.
9. Click **Activate Changes**
10. Restart the domain.
11. Repeat for the second domain

10.3.2 Update Server Start Parameters

As a workaround for a known issue in the 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. (The Console URLs are provided in Section 15.2, "About Identity and Access Management Console URLs.")
2. Navigate to **Environment -> Servers**.
3. Click **Lock and Edit**.
4. Click on the server **WLS_OIM1**.

5. Click on 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**.

10.4 Post-Deployment Steps for the Email Server

If you configured an email server in Section 8.12, "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 the **IAMGovernanceDomain** admin server and the OIM Managed Servers (**wls_oim1/2**).
   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 this 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|.oracle.com"
```

   For 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 this references from setDomainEnv.sh:

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

   c. Restart both the Administration and the Managed server.

10.5 Post-Deployment Steps for Access Manager

This section contains the following topics

- Section 10.5.1, "Update Idle Timeout Value"
- Section 10.5.2, "Update WebGate Agents"

10.5.1 Update Idle Timeout Value

By default the Access Manager idle timeout is set to two hours. This can cause issues with not being logged out after a session has timed out. Update this value to 15 minutes.

To update the idle timeout value:

1. Log in to the Access Management Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Log in as the Access Manager administrator user you created in Section 8.9, "Set User Names and Passwords" for example: `oamadmin`.
3. Click on **Common Settings** under **Configuration**.
4. Change **Idle Time out (minutes)** to `15`.
5. Click **Apply**.

10.5.2 Update WebGate Agents

After deployment, update existing WebGate Agents. The Identity and Access Management Console URLs are provided in Section 15.2, "About Identity and Access Management Console URLs."

Update the Access Manager Security Model of all WebGate profiles, with the exception of Webgate_IDM and Webgate_IDM_11g, which should already be set. In addition, set a password for the `IAMSuiteAgent` profile so that it can be used for OAAM for integration. (The `IAMSuiteAgent` was created when Access Manager was installed.)

To update these WebGate agents:

1. Log in to the Access Management Console as the Access Management administrator user identified by the entry in Section 8.9, "Set User Names and Passwords."
2. Click **SSO Agents** in the **Access Manager** box.
3. Ensure that the **WebGates** tab is selected.
4. Click **Search**.
5. Click an Agent, for example: **IAMSuiteAgent**.
6. Set the Security value to the same value defined to **OAM Transfer Mode** on the Access Manager Configuration screen in Section 8.15, "Configure Oracle Access Manager."

   Click Apply.
7. In the **Primary Server** list, click **+** and add any missing Access Manager Servers.
8. If a password has not already been assigned, enter a password into the **Access Client Password Field** and click **Apply**.

   Assign an Access Client Password, such as the **Common IAM Password** (*`COMMON_IDM_PASSWORD`*) you used in Section 8.9, "Set User Names and Passwords" or an Access Manager-specific password, if you have set one.
9. Set **Maximum Number of Connections** to 20 for all of the Access Manager Servers listed in the primary servers list. (This is the total maximum number of connections for the primary servers, which is 10 x WLS_OAM1 connections plus 10 x WLS_OAM2 connections.)
10. If you see the following in the **User Defined Parameters**:

```
logoutRedirectUrl=http://OAMHOST1.mycompany.com:14100/oam/server/logout
```

Change it to:

```
logoutRedirectUrl=https://sso.mycompany.com/oam/server/logout
```

11. Click **Apply**.
12. Repeat Steps through for each WebGate.
13. Check that the security setting matches that of your Access Manager servers.

10.6 Adding a Load Balancer Certificate to Trust Stores

Oracle Privileged Account Manager (OPAM) requires that the SSL certificate used by the load balancer be added to the trusted certificates in the JDK used by OPAM.

To add the certificate:

1. Obtain the certificate from the load balancer.

   You can obtain the load balancer certificate from the using a browser, such as Firefox. However, the easiest way to obtain the certificate is to use the `openssl` command. The syntax of the command is as follows:

   ```
   openssl s_client -connect LOADBALANCER -showcerts </dev/null
   2>/dev/null|openssl x509 -outform PEM > SHARED_CONFIG_
   DIR/keystores/sso.mycompany.com.pem
   ```

   For example:

   ```
   openssl s_client -connect sso.mycompany.com:443 -showcerts </dev/null
   2>/dev/null|openssl x509 -outform PEM > SHARED_CONFIG_
   DIR/keystores/sso.mycompany.com.pem
   ```

   This command saves the certificate to a file called `sso.mycompany.com.pem` in the following directory:

   ```
   SHARED_CONFIG_DIR/keystores
   ```

2. Load the certificate into the JDK and Node Manager Trust Stores by running the following command to import the CA certificate file, `sso.mycompany.com.pem`, into the *IGD_MW_HOME* Java, and Node Manager trust stores:

   ```
   set JAVA_HOME to IGD_MW_HOME/jdk6
   set PATH to include JAVA_HOME/bin

   keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
   -trustcacerts -keystore $JAVA_HOME/jre/lib/security/cacerts

   keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
   -trustcacerts -keystore
   SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1vhn.mycompany.com.jks

   keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
   -trustcacerts -keystore
   SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2vhn.mycompany.com.jks

   keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
   -trustcacerts -keystore
   SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1.mycompany.com.jks

   keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
   -trustcacerts -keystore
   ```

SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2.mycompany.com.jks

Where JAVA_HOME is set to IGD_MW_HOME/jdk6

You are prompted to enter a password for the keystore. The default password for the JDK is `changeit` and the `COMMON_IAM_PASSWORD` for the node manager keystores. You are also prompted to confirm that the certificate is valid.

Note: The names of the virtual hosts you assigned to your OIM server are `oimhost1vhn` and `oimhost2vhn`.

10.7 Restarting All Components

Restart all components, as described in Section 15.1, "Starting and Stopping Components."

11 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:

11.1 Validating the Administration Server

Validate the WebLogic Administration Server as follows.

11.1.1 Verify Connectivity

Verify that you can access the WebLogic Administration Console by accessing the following URLs and logging in as the user `weblogic_idm`:

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

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

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

Verify that you can access Oracle Enterprise Manager Fusion Middleware Control by accessing the URLs and logging in as the user `weblogic_idm`:

`http://IADADMIN.mycompany.com/em`

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

11.1.2 Validating Failover

Test failover of the Access Administration server to OAMHOST2, and then fall back to OAMHOST1 as described in Section 15.8, "Manually Failing Over the WebLogic Administration Server."

Test failover of the Identity Governance Administration server to OIMHOST2, and then fall back to OIMHOST1 as described in Section 15.8, "Manually Failing Over the

WebLogic Administration Server."

11.2 Validating the Access Manager Configuration

To Validate that this has completed correctly.

1. Access the Access Management Console at:
   `http://IADADMIN.mycompany.com/oamconsole`
2. Log in as the `oamadmin` user or the user identified by the entry in Section 8.9, "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`.

11.3 Validating Oracle Identity Manager

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Self Service Console in a Web browser at the following URL:

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

`https://igdadmin.mycomapany.com/identity`

Log in using the `xelsysadm` username and password.

11.4 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.

11.5 Validating Oracle Unified Directory

After configuration, you can validate that Oracle Unified Directory is working by performing a simple search. To do this issue the following commands:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAPHOST1.mycompany.com -p 1389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl

OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAPHOST2.mycompany.com -p 1389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl

OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h IDSTORE.mycompany.com -p 389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl
```

If Oracle Unified Directory is working correctly, you will see a list supportedControl entries returned.

To check that Oracle Unified Directory replication is enabled, issue the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/status
```

If you are asked how you wish to trust the server certificate, valid options are:

- Automatically trust
- Use a truststore
- Manually validate

Select your choice.

You are then prompted for the Administrator bind DN (`cn=oudadmin`) and its password.

Next, you see output similar to the following example. Replication will be set to enable.

```
--- Server Status ---
Server Run Status: Started
Open Connections: 2

--- Server Details ---
Host Name: ldaphost1
Administrative Users: cn=oudadmin
Installation Path: /u01/oracle/products/dir/oud
Instance Path: /u02/private/oracle/config/instances/oud1/OUD
Version: Oracle Unified Directory 11.1.2.2.0
Java Version: 1.6.0_29
Administration Connector: Port 4444 (LDAPS)

--- Connection Handlers ---
Address:Port : Protocol : State
-------------:-------------:---------
-- : LDIF : Disabled
8989 : Replication : Enabled
0.0.0.0:161 : SNMP : Disabled
0.0.0.0:1389 : LDAP : Enabled
0.0.0.0:1636 : LDAPS : Enabled
0.0.0.0:1689 : JMX : Disabled

--- Data Sources ---
Base DN: dc=mycompany,dc=com
Backend ID: userRoot
Entries: 1
Replication: Enabled
Missing Changes: 0
Age Of Oldest Missing Change: <not available>
```

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

To validate that WebGate is functioning correctly, open a web browser and go the Access Management Console at: `http://IADADMIN.mycompany.com/oamconsole`

You now see the Access Manager Login page displayed. Enter your Access Manager administrator user name (for example, `oamadmin`) and password and click **Login**. The Access Management console appears.

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`

Single Sign-On login page displays. Provide the credentials for the `weblogic_idm` user to log in.

11.7 Validating the Deployment

The following is a series of tests which you can perform to gain extra confidence in the deployment.

Testing SSO

Login to the Oracle Identity Manager Self Service Console using the URL as the user `xelsysadm`:

`https://sso.mycompany.com/identity` as `xelsysadmn`

Now try logging into the OIM System Administration console using the following URL:

`http://igdadmin.mycompany.com/sysadmin`

You should not be prompted to enter `xelsysadm` credentials again as you have already logged into the OIM Self Service console in the previous step.

Creating a New User in OUD to be Used by OAM

To create a new user in OUD:

1. Log in to the Oracle Identity Management Self Service console as `xelsysadmin` using the following URL:

   `http://sso.mycompany.com:443/identity`

2. Click on Users under Administration
3. Select Create from the Actions menu
4. Complete the information about the user on the displayed form and click Submit.
5. Click Sign Out.
6. Log in to the Oracle Identity Management Self Service console as the newly created user using the following URL:

   `http://sso.mycompany.com:443/identity`

   You are to set challenge questions at the first login. This indicates that the user was added to OUD and that you can log into OIM using OAM.

Testing the SOA workflow for approvals

To test the SOA workflow for approvals:

1. Access a protected resource, such as:

   `http://igdadmin.mycompany.com/sysadmin`

2. Click **Register New Account**.
3. Complete information about the new account and click **Register**
4. Click **Return**, then make a note of the request number.
5. Log in to the Oracle Identity Management Self Service console as the user `xelsysadm`.
6. Click **Inbox**.
7. You request appears in the list of Pending approvals.
8. Click on the request and select **Approve** from the **Actions** menu.

9. Log out of the Identity Management Self Service console.
10. Log back in as the newly created user.

12

Extending the Domain to Include Oracle Adaptive Access Manager

This chapter describes the procedure to extend an Identity and Access Management domain to include Oracle Adaptive Access Manager.

This chapter contains the following topics:

12.1 Overview of Extending the Domain to Include OAAM

Oracle Adaptive Access Manager (OAAM) is built on a Java EE-based, multi-tiers deployment architecture that separates the platform's presentation, business logic, and data tiers. Because of this separation of tiers, OAAM can rapidly scale with the performance needs of the customer. The architecture can leverage the most flexible and supported cross-platform Java EE services available: a combination of Java, XML and object technologies. This architecture makes OAAM a scalable, fault-tolerant solution.

Oracle Adaptive Access manager consists of the following two components.

- OAAM Administration Applications
- OAAM Server Applications

12.2 OAAM Details

Use this worksheet to keep track of OAAM information

Table 12–1 OAAM Details

Description	Documented Variable	Documented Value	Customer Value
OAAM Managed Server Names		wls_oaam1 wls_oaam2	
OAAM Managed Server Port	*OAAM_PORT*	14300	
OAAM Managed Server SSL Port	*OAAM_SSL_PORT*	14301	
OAAM Administrative Managed Server Names		wls_oaam_admin1 wls_oaam_admin2	
OAAM Administrative Managed Port	*OAAM_ADMIN_PORT*	14200	
OAAM Administrative Managed SSL Port	*OAAM_ADMIN_SSL_PORT*	14201	
Identity Store Host	*LDAP_HOST*	LDAPHOST1.mycompany.com	
Identity Store Port	*LDAP_PORT*	1389	
Identity Store Bind DN	*LDAP_ADMIN_USER*	cn=oudadmin	
Identity Store Administrator Port	*LDAP_DIR_ADMIN_PORT*	4444	
Identity Store Group Search Base	*LDAP_GROUP*	cn=Groups,dc=mycompany,dc=com	
OAAM Administrative User	*OAAMADMINUSER*	oaamadmin	
Access Manager Host1 (Consolidated)	*OAMHOST1*	IAMHOST1	
Access Manager Host2 (Consolidated)	*OAMHOST2*	IAMHOST2	
Access Manager Host1 (Distributed)	*OAMHOST1*	OAMHOST1	
Access Manager Host2 (Distributed)	*OAMHOST2*	OAMHOST2	

Note: Only one LDAPHOST needs to be specified and it should not be the LDAP load balancer name.

12.3 Prerequisites

The instructions in the following subsections are for the distributed mode. If you are using the consolidated deployments, references to OAMHOST1 and OAMHOST2

should be replaced by IAMHOST1 and IAMHOST2, as shown in Table 12–1.

Before you extend the domain to include Oracle Adaptive Access Manager (OAAM), the following prerequisites must be in place.

12.3.1 Creating a Highly Available Database

Create a highly available database to hold the OAAM data, if you are not using the IAMDB. Pre-seed the database with OAAM data objects using the repository creation utility as described in Section 6.5, "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU."

12.3.2 Creating OAAM Users and Groups in LDAP

Create OAAM Users and Groups as follows:

Create a configuration file with the following contents:

```
# Common
IDSTORE_HOST: LDAPHOST1.mycompany.com
IDSTORE_PORT: 1389
IDSTORE_ADMIN_PORT: 4444
IDSTORE_BINDDN: cn=oudadmin
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=mycompany,dc=com
IDSTORE_OAAMADMINUSER: oaamadmin
```

Where:

- `IDSTORE_HOST` (*`LDAP_HOST`*) and `IDSTORE_PORT` (*`LDAP_PORT`*) are, respectively, the host and port of your Identity Store directory, for example:

  OUD: `LDAPHOST1` and `1389`

- `IDSTORE_ADMIN_PORT` (*`LDAP_DIR_ADMIN_PORT`*) is the administration port of your Oracle Unified Directory instance.

- `IDSTORE_BINDDN` (*`LDAP_ADMIN_USER`*) is an administrative user in the Identity Store Directory.

- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where groups are stored. This is composed of `cn=Groups` combined with the *`REALM_DN`* defined in Section 7.1, "Assembling Information for Identity and Access Management Deployment," for example: `cn=Groups,dc=mycompany,dc=com`

- `IDSTORE_SEARCHBASE` is the location in the directory where users and groups are stored. This is the same as the *`REALM_DN`* defined in Section 7.1, "Assembling Information for Identity and Access Management Deployment," for example: `cn=Users,dc=mycompany,dc=com`

- `IDSTORE_USERNAMEATTRIBUTE` is the name of the directory attribute containing the user's name, for example: `cn`. Note that this is different from the login name.

- `IDSTORE_LOGINATTRIBUTE` is the LDAP attribute which contains the users Login name, for example: `uid`.

- `IDSTORE_USERSEARCHBASE` is the location in the directory where users are stored. This is composed of `cn=Users` combined with the *`REALM_DN`* defined in Section 7.1,

"Assembling Information for Identity and Access Management Deployment," for example: `dc=mycompany,dc=com`

- `IDSTORE_OAAMADMINUSER` (*`OAAMADMINUSER`*) is the name of the user you want to create as your Oracle Adaptive Access Manager Administrator.

Create users using `idmConfigTool`.

You must seed the Identity Store with users and groups that are required by the Identity and Access Management components. To seed users and groups in Identity Store, perform the following tasks on OAMHOST1:

1. Set environment variables.
   - Set *`MW_HOME`* to `IAD_MW_HOME`.
   - Set *`ORACLE_HOME`* to `IAD_ORACLE_HOME`.
   - Set *`JAVA_HOME`* to `JAVA_HOME`.
2. Configure the Identity Store by using the command `idmConfigTool`, which is located at: *`IAD_ORACLE_HOME`*`/idmtools/bin`

   The syntax of the command on Linux is:

   ```
   idmConfigTool.sh -prepareIDStore mode=OAAM input_file=configfile
   ```

Where `configfile` is the name of the configuration file you created at the beginning of this section.

3. When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with.

   During the command execution you are prompted to supply passwords for the accounts being created. For ease of use, it is recommended that you supply the `COMMON_IDM_PASSWORD` if you are using a common password throughout.

   After running each command, check the log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory where you run the tool.

12.4 Extending Domain for Oracle Adaptive Access Manager

Start the configuration wizard by executing the following command on *`OAMHOST1`*:

```
IAD_MW_HOME/oracle_common/common/bin/config.sh
```

Then proceed as follows:

1. On the Welcome Screen, select **Extend an Existing WebLogic Domain**. Click **Next**
2. On the Select a WebLogic Domain screen, using the navigator select the domain home of the Administration Server, for example: *`IAD_ASERVER_HOME`* (IAMAccessDomain)

   Click **Next**.
3. On the Select Extension Source screen, select the following:
   - **Oracle Adaptive Access Manager - Server**
   - **Oracle Adaptive Access Manager - Admin Server**

   Click **Next**
4. On the Configure JDBC Component Schema screen, do the following:

Select:

- OAAM Admin Schema
- OAAM Server Schema
- OAAM Admin MDS Schema
- OWSM MDS Schema

For the Oracle RAC configuration for component schemas, select **Convert to GridLink**.

Click **Next**.

5. The Gridlink RAC Component Schema screen appears. In this screen, enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU. For Exadata SDP Connections, enter the TCP parameters below. Later, this must be converted to an SDP Connect String.
   - **Driver**: Select Oracle's driver (Thin) for GridLink Connections,Versions:10 and later.
   - Select **Enable FAN**.
   - Do one of the following:
     - If SSL is not configured for ONS notifications to be encrypted, deselect **SSL**.
     - Select **SSL** and provide the appropriate wallet and wallet password.
   - **Service Listener**: Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the parameter `remote_listener` in the database:

```
SQL>show parameter remote_listener;

NAME            TYPE   VALUE
-----------------------------------------------------------
remote_listener string iamdbscan.mycompany.com:1521
```

Note:

For Oracle Database 11*g* Release 1 (11.1), use the virtual IP and port of each database instance listener, for example:
`DBHOST1-VIP.mycompany.com` (port `1521`) and
`DBHOST2-VIP.mycompany.com` (port `1521`), where `1521` is *`DB_LSNR_PORT`*

   - **ONS Host**: Enter the SCAN address for the Oracle RAC database and the ONS remote port as reported by the database:

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

Note: For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

```
DBHOST1.mycompany.com (port 6200)
```

and

```
DBHOST2.mycompany.com (port 6200)
```

Enter the following RAC component schema information:

Schema Name	Service Name	Schema Owner	Password
OAAM Admin Schema	oaamedg.mycompany.com	EDGIAD_OAAM	*password*
OAAM Admin MDS Schema	oaamedg.mycompany.com	EDGIAD_MDS	*password*
OAAM Server Schema	oaamedg.mycompany.com	EDGIAD_OAAM	*password*
OWSM MDS Schema	oamedg.mycompany.com	EDGIAD_MDS	*password*

6. On the Test Component Schema screen, the configuration wizard attempts to validate the data source. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the issue, and try again.
7. On the Select Optional Configuration screen, select **Managed Server Clusters and Machines**. Click **Next**
8. When you first enter the Configure Managed Servers screen, you will see entries for components already configured such as Access Manager. In addition the wizard will create 2 new managed servers for OAAM.

Note: When you first enter this screen the config wizard has created default Managed Servers for you.

Change the details of the default Managed Server to reflect the following details. That is, ***change one entry and add one new entry***.

Do not change the configuration of any Managed Servers which have already been configured as part of previous application deployments.

Default Name	Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
oaam_server_server1	wls_oaam1[1]	*OAMHOST1*	14300 (*OAAM_ADMIN_PORT*)[2]	14301 (*OAAM_ADMIN_SSL_PORT*)	Selected
	wls_oaam2	*OAMHOST2*	14300 (*OAAM_ADMIN_PORT*)	14301 (*OAAM_ADMIN_SSL_PORT*)	Selected
oam_admin_server1	wls_oaam_admin1	*OAMHOST1*	14200 (*OAAM_PORT*)	14201 (*OAAM_SSL_PORT*)	Selected
	wls_oaam_admin2	*OAMHOST2*	14200 (*OAAM_PORT*)	14201 (*OAAM_SSL_PORT*)	Selected

[1] You MUST use the names listed in the table to facilitate automated patching.

[2] See Section B.3.

Leave all other fields at the default settings and click **Next**.

9. On the Configure Clusters screen, create a cluster by clicking **Add** and provide the values shown for oaam_cluster in the following table. Then create a second cluster by clicking Add and provide the values shown for oaam_admin_cluster in the table.

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
oaam_cluster	unicast	n/a	n/a	Leave it empty.
oaam_admin_cluster	unicast	n/a	n/a	Leave it empty.

Leave all other fields at the default settings and click **Next**.

10. On the Assign Servers to Clusters screen, associate the Managed Servers with the cluster. Click the cluster name in the right pane. Click the Managed Server under **Servers**, then click the arrow to assign it to the cluster.

Assign servers to the clusters as follows:

Cluster	Server
oaam_cluster	wls_oaam1
	wls_oaam2
oaam_admin_cluster	wls_oaam_admin1
	wls_oaam_admin2

> **Note:** Do not change the configuration of any clusters which have already been configured as part of previous application deployments.

Click **Next**.

11. On the Configure Machines screen, click **Next**.

> **Note:** Deployment will have created Machines for you

12. On the Assign Servers to Machines screen, assign servers to machines as follows:
    - **OAMHOST1**: **wls_oaam1**, **wls_oaam_admin1**
    - **OAMHOST2**: **wls_oaam2**, **wls_oaam_admin2**

    Click **Next** to continue.

13. On the Configuration Summary screen, click **Extend** to extend the domain.

Note: Note: If you receive a warning that says:

```
CFGFWK: Server listen ports in your domain configuration conflict
with ports in use by active processes on this host
```

Click **OK**.

This warning appears if Managed Servers have been defined as part of previous installs and can safely be ignored.

12.5 Restarting Administration Server on OAMHOST1

Restart WebLogic Administration Server on OAMHOST 1. See Section 15.1, "Starting and Stopping Components."

12.6 Deploying Managed Server Configuration to Local Storage

Once the configuration is complete, you must propagate the Oracle Adaptive Access Manager configuration to the managed server directory on OAMHOST1 and OAMHOST2.

Propagate the Oracle Adaptive Access Manager by packing first the domain `IAMAccessDomain` from the shared storage location and unpacking it to managed server directory on local storage.

You do this by packing and unpacking the domain, you pack the domain first on IAMAccessDomain on OAMHOST1 then unpack it on OAMHOST1 and OAMHOST2.

Follow these steps to propagate the domain to the managed server domain directory.

1. Invoke the `pack` utility from *`ORACLE_COMMON_HOME`*`/common/bin/` on OAMHOST1.

   ```
   ./pack.sh -domain=IAD_ASERVER_HOME -template=iam_domain.jar  -template_
   name="IAM Domain" -managed=true
   ```

   This creates a file called `iam_domain.jar`. Copy this file to OAMHOST2.

2. On OAMHOST1 and OAMHOST2, invoke the utility `unpack`, which is also located in the directory: *`ORACLE_COMMON_HOME`*`/common/bin/`

   ```
   ./unpack.sh -domain=IAD_MSERVER_HOME -template=iam_domain.jar -overwrite_
   domain=true -app_dir=IAD_MSERVER_HOME/applications
   ```

   If you see a message similar to this, you may safely ignore it:

   ```
   ------------------------------------------------------------
   >>  Server listen ports in your domain configuration conflict with ports in use
   by active processes on this host.
   Port 14100 on wls_oam2
   ------------------------------------------------------------------
   ```

12.7 Adding OAAM Servers to Start and Stop Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. Whenever you create a new managed server in the domain you must update the domain configuration so that these start and stop scripts can also start the newly created managed server. You must now do this for each of the OAAM managed servers.

To update the domain configuration, edit the file `serverInstancesCustom.txt`, which is located in the directory: *`SHARED_CONFIG_DIR`*`/scripts`

If you want to start a node manager on a new machine, add an entry which looks like this:

```
newmachine.mycompany.com NM nodemanager_pathname nodemanager_port
```

For example:

```
OAMHOST3.mycompany.com NM /u01/oracle/config/nodemanager/oamhost3.mycompany.com
5556
```

For each of the OAAM managed servers in the table in Section 12.4, "Extending Domain for Oracle Adaptive Access Manager", Step 8 (Configure Managed Servers screen), add an entry which looks like this:

```
newmachine.mycompany.com OAAM ManagedServerName
```

For example:

```
OAMHOST1 OAAM wls_oaam1 IADADMINVHN 7001
OAMHOST1 OAAM wls_oaam_admin1 IADADMINVHN 7001
OAMHOST2 OAAM wls_oaam2 IADADMINVHN 7001
OAMHOST2 OAAM wls_oaam_admin2 IADADMINVHN 7001
```

Save the file.

12.8 Starting and Validating OAAM on OAMHOST1

This section contains the following topics:

- Section 12.8.1, "Starting Oracle Adaptive Access Manager on OAMHOST1"
- Section 12.8.2, "Validating OAAM on OAMHOST1"

12.8.1 Starting Oracle Adaptive Access Manager on OAMHOST1

Start the WebLogic Administration Console for `IAMAccessDomain` using the URL specified in Section 15.2, "About Identity and Access Management Console URLs."

Select **Environment**, **Servers** from the domain structure menu then click the **Control** tab.

Select the servers wls_oaam_admin1 and wls_oaam1 and click **Start**.

12.8.2 Validating OAAM on OAMHOST1

Validate the implementation by connecting to the OAAM Administration Server at:

```
http://OAMHOST1.mycompany.com:14200/oaam_admin
```

and to the OAAM server at:

```
http://OAMHOST1.mycompany.com:14300/oaam_server
```

The implementation is valid if the OAAM Server login page is displayed and you can log in using the `oaamadmin` account you created in Section 12.3.2, "Creating OAAM Users and Groups in LDAP."

12.9 Starting and Validating OAAM on OAMHOST2

This section describes how to configure Oracle Adaptive Access Manager on OAMHOST2.

This section contains the following topics:

- Section 12.9.1, "Starting Oracle Adaptive Access Manager on OAMHOST2"
- Section 12.9.2, "Validating OAAM on OAMHOST2"

12.9.1 Starting Oracle Adaptive Access Manager on OAMHOST2

Start Oracle Adaptive Access Manager on OAMHOST2 by following the start procedures in Section 15.1, "Starting and Stopping Components" for WebLogic Managed Servers wls_oaam2 and wls_oaam_admin2.

12.9.2 Validating OAAM on OAMHOST2

Validate the implementation by connecting to the OAAM Administration Server at `http://OAMHOST2.mycompany.com:14200/oaam_admin`. The implementation is valid if OAAM Administration console login page is displayed and you can login using the `oaamadmin` account you created in Section 12.3.2, "Creating OAAM Users and Groups in LDAP."

Validate the implementation by connecting to the OAAM Server at: `http://OAMHOST2.mycompany.com:14300/oaam_server` The implementation is valid if the OAAM Server login page is displayed.

12.10 Configuring OAAM to Work with Web Tier

This section describes how to configure Oracle Adaptive Access Manager to work with the Oracle HTTP Server.

This section contains the following topics:

- Section 12.10.1, "Configuring Access from Oracle HTTP Server"
- Section 12.10.2, "Changing Host Assertion in WebLogic"
- Section 12.11, "Loading Oracle Adaptive Access Manager Seed Data"
- Section 12.10.3, "Validating Oracle Adaptive Access Manager"

12.10.1 Configuring Access from Oracle HTTP Server

You must include OAAM in the Web Tier configuration by updating the following files on WEBHOST1 and WEBHOST2:

12.10.1.1 Updating IADADMIN.mycompany.com

Add the following to *`WEB_ORACLE_INSTANCE`*`/config/OHS/component_name/moduleconf/idmadmin_vh.conf`:

```
#####################################################
## Entries Required by Oracle Adaptive Access Manager
#####################################################

   # OAAM Console
   <Location /oaam_admin>
      SetHandler weblogic-handler
```

```
   WebLogicCluster OAMHOST1.mycompany.com:14200,OAMHOST2.mycompany.com:14200
</Location>
```

12.10.1.2 Updating sso.mycompany.com

Add the following to *WEB_ORACLE_INSTANCE*/config/OHS/component_name/moduleconf/sso_vh.conf:

```
#####################################################
## Entries Required by Oracle Adaptive Access Manager
#####################################################

<Location /oaam_server>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.mycompany.com:14300,OAMHOST2.mycompany.com:14300
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>
```

12.10.1.3 Restarting Oracle HTTP Servers and OAAM Managed Servers

Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2, as described in Section 15.1, "Starting and Stopping Components."

Restart the managed servers wls_oaam1, wls_oaam2, wls_oaam_admin1, and wls_oaam_admin2 as described in Section 15.1, "Starting and Stopping Components."

12.10.2 Changing Host Assertion in WebLogic

Because the Oracle HTTP Server acts as a proxy for WebLogic, by default certain CGI environment variables are not passed through to WebLogic. These include the host and port. You must tell WebLogic that it is using a virtual site name and port so that it can generate internal URLs appropriately.

To do this, log in to the WebLogic administration console in the IAMAccessDomain at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."

Then proceed as follows:

1. Select **Clusters** from the home page or, alternatively, select **Environment** -> **Clusters** from the Domain structure menu.
2. Click **Lock and Edit** in the Change Center Window to enable editing.
3. Click the Cluster Name (**oaam_cluster**).
4. Select **HTTP** and enter the following values (from Section 7.1, "Assembling Information for Identity and Access Management Deployment"):
   - **Frontend Host**: `sso.mycompany.com` (*IAM_LOGIN_URI*)
   - **Frontend HTTP Port:** `80` (*HTTP_PORT*)
   - **Frontend HTTPS Port:** `443` (*HTTP_SSL_PORT*)

   This ensures that any HTTPS URLs created from within WebLogic are directed to port 443 on the load balancer.
5. Click **Save**.
6. Select **Clusters** from the home page or, alternatively, select **Environment** -> **Clusters** from the Domain structure menu.

7. Click the Cluster Name (**oaam_admin_cluster**).
8. Select HTTP and enter the following values (from Section 7.1, "Assembling Information for Identity and Access Management Deployment"):
   - **Frontend Host**: `IADADMIN.mycompany.com` (*IAD_DOMAIN_ADMIN_LBRVHN*)
   - **Frontend HTTP Port**: `80` (*HTTP_PORT*)
9. Click **Save**.
10. Click **Activate Changes** in the Change Center window to enable editing.

12.10.3 Validating Oracle Adaptive Access Manager

Log in to the Oracle Adaptive Access Management Administration console, at the URL listed in Section 15.2, "About Identity and Access Management Console URLs," using the `oaamadmin` account you created in Section 13.5.2, "Creating OAAM Administration User in WebLogic Console."

Also log in to the Oracle Adaptive Access Manager server at `https://sso.mycompany.com/oaam_server` in using the account `oaamadmin` account and the password `test`.

Check that the following URL can be accessed:

`https://sso.mycompany.com:443/oaam_server/oamLoginPage.jsp`

12.11 Loading Oracle Adaptive Access Manager Seed Data

This section describes how to load seed data into Oracle Adaptive Access Manager.

> **Note:** Either copy the files from OAMHOST1 to your local machine (where you are running the browser) or run this step from a browser started on OAMHOST1.

1. Log in to Oracle Adaptive Access Management Administration console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."

   Connect using the `oaamadmin` account that you created in Section 12.3.2, "Creating OAAM Users and Groups in LDAP."
2. Click **System Snapshots**, which is located on the **Navigation -> Environment** menu.

   Click **Open**.
3. Click **Load From File**.
4. Enter the following information:
   - **Name**: `Default Snapshot`
   - **Notes**: `Default Snapshot`

   Select **Backup Current System Now**.

   Click **Continue**.
5. Click **OK** to acknowledge backup creation.
6. Click **Choose File.**
7. Select the file `oaam_base_snapshot.zip` which is located in:

IAD_ORACLE_HOME/oaam/init

8. Click **Load**.

   You will see a message that says that the snapshot file was loaded successfully. Acknowledge this message by clicking **OK**.

9. Click **Restore** near the top right.

10. When loading is complete, a message is displayed. Click **OK**.

12.12 Integrating Oracle Adaptive Access Manager with Oracle Access Management Access Manager

This section describes how to integrate OAAM with Access Manager and Oracle Identity Manager. Once OAAM has been integrated with Access Manager, you can use OAAM instead of the standard Access Manager login to validate access to resources. Even though OAAM is performing the authentication, it is authenticating against users in Access Manager.

When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

This section contains the following topics:

- Section 12.12.1, "Retrieving the Global Passphrase for Simple Mode."
- Section 12.12.2, "Registering OAAM as a Third Party Application."
- Section 12.12.3, "Validation."
- Section 12.12.4, "Setting OAAM properties for Access Manager."
- Section 12.12.5, "Creating a Test Resource."
- Section 12.12.6, "Validating Oracle Adaptive Access Manager."
- Section 12.12.7, "Moving TAP Resource to LDAP Policy,"

12.12.1 Retrieving the Global Passphrase for Simple Mode

Access Manager generates a random global passphrase for Simple mode communication during installation. The following procedure describes how to retrieve this passphrase. You will need it later in this chapter.

To retrieve the random global passphrase for Simple mode communication, on OAMHOST1 invoke the WebLogic Scripting Tool located in *IAD_ORACLE_HOME*/common/bin. Once you are in the wlst shell, enter the command to connect.

```
./wlst.sh
wls:/offline> connect()
```

Respond to the prompts as shown:

```
Please enter your username [weblogic] : weblogic
Please enter your password [weblogic] : COMMON_IDM_PASSWORD
Please enter your server URL [t3://localhost:7001] : t3://IADADMINVHN:7001
wls:/IAMAccessDomain/serverConfig>
```

Enter the following command to change the location to the read-only domainRuntime tree. For help, use help(domainRuntime)).

```
wls:/IAMAccessDomain/domainRuntime>domainRuntime()
```

View the global passphrase by entering the following command.

```
wls:/IAMAccessDomain/domainRuntime> displaySimpleModeGlobalPassphrase()
```

Make a note of this passphrase and exit `wlst` by using the `exit` command:

```
wls:/IAMAccessDomain/domainRuntime> exit()
```

12.12.2 Registering OAAM as a Third Party Application

If you have configured Access Manager to use the Simple Security Transportation protocol, you must register OAAM as a third-party application.

To register OAAM as a third-party application:

1. Create a directory to hold the OAAM Keystore. Placing this directory in the *IAD_ASERVER_HOME* ensures that it is available to all OAAM Hosts.

   ```
   mkdir -p IAD_ASERVER_HOME/keystores
   ```

2. From OAMHOST1, start the WLST shell from the *IAD_ORACLE_HOME*`/common/bin` directory. For example, on Linux, you would type:

   ```
   ./wlst.sh
   ```

3. Connect to the WebLogic Administration Server using the following `wlst` connect command:

   ```
   connect('AdminUser',"AdminUserPassword",t3://hostname:port')
   ```

   For example:

   ```
   connect("weblogic","admin_password","t3://IADADMINVHN.mycompany.com:7001")
   ```

4. Run the `registerThirdPartyTAPPartner` command as follows:

   ```
   registerThirdPartyTAPPartner(partnerName = "partnerName", keystoreLocation=
   "path to keystore" , password="keystore password", tapTokenVersion="v2.0",
   tapScheme="TAPScheme", tapRedirectUrl="OAAM login URL")
   ```

   For example:

   ```
   registerThirdPartyTAPPartner(partnerName = "OAAMTAPPartner", keystoreLocation=
   "IAD_ASERVER_HOME/keystores/oaam_keystore.jks" , password="password",
   tapTokenVersion="v2.0", tapScheme="TAPScheme",
   tapRedirectUrl="https://sso.mycompany.com/oaam_server/oamLoginPage.jsp")
   ```

   Where:

   - `partnerName` is a unique name. If the partner exists in Access Manager, the configuration will be overwritten.
   - `keystoreLocation` is an existing Key Store location. If the directory path you specified is not present, you get an error.
   - `password` is the password specified to encrypt the key store. Remember this, as you will need it later.
   - `tapTokenVersion` is always `v2.0`.
   - `tapScheme` is the authentication scheme to be updated.
   - `tapRedirectUrl` is a reachable URL. If it is not, registration fails with the message: `Error! Hyperlink reference not valid`.

Note: Due to a bug, `tapRedirectURL` must be an HTTP URL. This is changed to HTTPS later.

- `tapRedirectUrl` is:

  `https://sso.mycompany.com/oaam_server/oamLoginPage.jsp`

5. Exit WLST.

   `exit()`

6. Log in to the Access Management Administration Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
7. Click **Authentication Schemes** in the **Access Manager** section.

   The Search Authentication Schemes Page is displayed.

   Enter `TAPScheme` in the **Search Name** box and click **Search**.
8. Click **TAPScheme**.
9. Verify that the **Challenge URL** is set to:

   `/oaam_server/oamLoginPage.jsp`

   The parameters `TAPPartnerId=OAAMTAPPartner` and `SERVER_HOST_ALIAS=OAMSERVER` should already be listed as **Challenge Parameter**s. Add the following **Challenge Parameter**s:

   - `MatchLDAPAttribute=uid`
   - `TAPOverrideResource=https://sso.mycompany.com:443/oamTAPAuthenticate`
10. Click **Apply**.
11. Restart wls_oaam1 and wls_oaam2 as described in Section 15.1, "Starting and Stopping Components."

12.12.3 Validation

Use the OAM Access Tester tool to ensure that this integration has been completed successfully.

To ensure the integration is completed successfully:

1. Ensure that *JAVA_HOME* is set in your environment.
2. Add *JAVA_HOME*`/bin` to your *PATH*, for example:

   `export PATH=$JAVA_HOME/bin:$PATH`

3. Change directory to:

   IAD_ORACLE_HOME`/oam/server/tester`

4. Start the test tool in a terminal window using the command:

   `java -jar oamtest.jar`

5. Connect using the following values:

   - **Primary OAM Host**: `OAMHOST1`
   - **Port**: `5575` (*OAM_PROXY_PORT*)

- **Agent ID**: IAMSuiteAgent
- **Agent Password**: Password you assigned to the IAMSuiteAgent profile
- **Mode**: Select **Open** for AIX platforms. Otherwise, select **Simple**.
- **Global Passphrase**: If you selected Simple mode, enter the Access Manager global passphrase obtained in Section 12.12.1, "Retrieving the Global Passphrase for Simple Mode.".

Click **Connect**.

6. Provide Protected Resource URI:
   - **Scheme**: http
   - **Host**: IAMSuiteAgent
   - **Port**: Leave blank
   - **Resource**: /oamTAPAuthenticate

   Click **Validate**.
7. Provide User Identity oamadmin and the password for oamadmin.

   Click **Authenticate**. If the authentication is successful, integration has been completed successfully.

Perform the same validation on OAMHOST2.

12.12.4 Setting OAAM properties for Access Manager

Set the OAAM properties for Access manager by editing the oaam_cli.properties file.

To set the OAAM properties on OAMHOST1:

1. Copy *IAD_ORACLE_HOME*/oaam/cli to a temporary location. For example:

   ```
   cp -r IAD_ORACLE_HOME/oaam/cli /u01/oracle/oaam
   ```

2. Edit the file oaam_cli.properties, which is located in the directory:

   /u01/oracle/oaam/conf/bharosa_properties.

   Set the following property values in the file:

Parameter	Value
oaam.adminserver.hostname	IADADMINVHN.mycompany.com
oaam.adminserver.port	7001
oaam.adminserver.username	weblogic
oaam.adminserver.password	Password for the weblogic user
oaam.db.url	The DBC URL for the OAAM Database. Format: jdbc:oracle:thin:@(DESCRIPTION=(LOAD_ BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN) (PORT=1521))(CONNECT_DATA=(SERVICE_NAME=oaamedg.mycompany.com)))
oaam.uio.oam.tap.keystoreFile	The location of the keystore that was created in Section 12.12.2, "Registering OAAM as a Third Party Application."For example: *IAD_ASERVER_HOME*/keystores/oaam_keystore.jks
oaam.uio.oam.tap.partnername	OAAMTAPPartner

Parameter	Value
oaam.uio.oam.host	*OAMHOST1*
oaam.uio.oam.port	The Access Manager Server proxy port *OAM_PROXY_PORT*. For example: 5575.
oaam.uio.oam.webgate_id	IAMSuiteAgent
oaam.uio.oam.secondary.host	*OAMHOST2*
oaam.uio.oam.secondary.host.port	The Access Manager Server proxy port, *OAM_PROXY_PORT*, on the second Access Manager Server. For example: 5575.
oaam.uio.oam.security.mode	This depends on the Access Manager security transport mode in use. If this is an AIX build, then the value will be 1 (Open) otherwise it will be 2 (Simple).
oam.uio.oam.rootcertificate.keystore.filepath	The location of the Keystore file generated for the root certificate: *IAD_ASERVER_HOME*/output/webgate-ssl/oamclient-truststore.jks This is required only for security modes 2 (Simple) and 3 (Cert).
oam.uio.oam.privatekeycertificate.keystore.filepath	The location of the Keystore file generated for private key: *IAD_ASERVER_HOME*/output/webgate-ssl/oamclient-keystore.jks This is required for security modes 2 (Simple) and 3 (Cert).

Save the file

3. Execute the OAAM CLI tool by issuing the command setupOAMTapIntegration.sh, which is located in the directory:

   /u01/oracle/oaam

   as follows:

   Set ORACLE_MW_HOME to *IAD_MW_HOME*

   Set JAVA_HOME to *JAVA_HOME*

   Set WLS_HOME to *IAD_MW_HOME*/wlserver_10.3

   Set APP_SERVER_TYPE to weblogic

   Run the commands:

   ```
   chmod +x /u01/oracle/oaam/setupOAMTapIntegration.sh
   /u01/oracle/oaam/setupOAMTapIntegration.sh /u01/oracle/oaam/conf/bharosa_
   properties/oaam_cli.properties
   ```

   When the command runs, it prompts you for the following information:

   - OAAM AdminServer User Name: weblogic
   - OAAM AdminServer Password: Password for weblogic account
   - OAAM DB username: EDG_OAAM.
   - OAAM DB password: Password for the OAAM database user.
   - OAM Webgate Credentials to be stored in CSF: Enter WebGate password (*COMMON_IDM_PASSWORD*).
   - OAM TAP Key store file password: The password you assigned when you registered OAAM as a 3rd party application in Section 12.12.2, "Registering OAAM as a Third Party Application" (*COMMON_IDM_PASSWORD*).
   - OAM Private Key certificate Key store file password: The Access Manager global passphrase obtained in Section 12.12.1, "Retrieving the Global

Passphrase for Simple Mode."

- OAM Global Pass phrase: If you are using the OAAM Simple security model then this is the value retrieved in Section 12.12.1, "Retrieving the Global Passphrase for Simple Mode."

12.12.5 Creating a Test Resource

To perform this validation, first create a test resource.

Create a test page called `oaam_sso.html` on WEBHOST1 and WEBHOST2. The easiest way to do this is to create a file called `oaam_sso.html` in the directory *`WEB_ORACLE_INSTANCE`*`/config/OHS/`*`component`*`/htdocs` with the following:

```
<html>
<body>
<center>
<p>
<h2>
OAAM Protected Resource
</h2>
</p>
</center>
</body>
</html>
```

12.12.5.1 Creating Oracle Adaptive Access Manager Policies

Create a group for OAAM Protected resources in the IAMSuite Application Domain.

1. Log in to the Access Management Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs," using the `oamadmin` account created previously
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**. The IAM Suite Domain page is displayed.
5. Click the **Authentication Policies** tab.
6. Click **Create Authentication Policy** and enter the following information:
   - **Name**: `OAAM Protected Resources`
   - **Description**: `Resources protected by OAAM`
   - **Authentication Scheme**: TAPScheme
7. Click **Apply**.
8. Repeat Steps 1 through 7, but enter the following values after clicking Create Authentication Policy:
   - **Name**: `LDAP Protected Resource`
   - **Description**: `Resources protected by LDAPScheme`
   - **Authentication Scheme**: LDAPScheme

12.12.5.2 Creating a Resource in Access Manager

Now that you have something to protect, you must create a resource in Access Manager and assign it to one of the policy groups you just created.

1. Log in to the Access Management Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.
5. Click the **Resources** tab.
6. Click **New Resource** and enter the following information:
   - **Type**: `http`
   - **Description**: `OAAM Test Page`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/oaam_sso.html`
   - **Protection Level**: `Protected`
   - **Authentication Policy**: `OAAM Protected Resources`
   - **Authorization Policy**: `Protected Resource Policy`
7. Click **Apply**.

12.12.6 Validating Oracle Adaptive Access Manager

Access your protected resource using the URL: `https://sso.mycompany.com:443/oaam_sso.html`. You are redirected to OAAM for registration and challenge. The OAAM login page is shown instead of the Access Manager login page. Log in using an authorized Access Manager user such as `oamadmin`. Once you are logged in, the oaam protected resource is displayed.

12.12.7 Moving TAP Resource to LDAP Policy

1. Log in to the Access Management Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs," using the `oamadmin` account created previously.
2. Click on **Application Domains** under the **Access Manager** section.

   The Application Domains Search screen appears.

   Click **Search**.

   Click on **IAM** Suite to bring up the IAM Suite Domain page.

   Click on the **Authentication Policies** subtab.
3. Click **Protected Higher Level Policy**.
4. Click on the **Resources** subtab.
5. In the Resources window click **/oamTAPAuthenticate**.
6. Click **Delete**.
7. Click **Apply**.
8. Click on **Application Domains** under the **Access Manager** section.

   The Application Domains Search screen appears.

   Click **Search**.

Click on **IAM** Suite to bring up the IAM Suite Domain page.

Click on the **Authentication Policies** subtab.

9. Click **LDAP Protected Resources**.
10. Click **Open** on the tool bar below the **Browse** tab.
11. In the Resources window, click **Add**.

    When the Search box appears enter:

    Resource URL: `/oamTAPAuthenticate`

    Click **Search**.

    Click on **/oamTAPAuthenticate** from the search results.

    Click **Add Selected**.
12. Select the resource **/oamTAPAuthenticate**.
13. Click **Apply**.

12.13 Integrating Oracle Adaptive Access Manager 11*g* with Oracle Identity Manager 11*g*

OAAM provides a comprehensive set of challenge questions. Its functionality includes:

- Challenging the user before and after authentication, as required, with a series of questions.
- Presenting the questions as images and seeking answers through various input devices.
- Asking questions one after another, revealing subsequent questions only if correct answers are provided.

Oracle Identity Manager also has basic challenge question functionality. It enables users to answer a set of configurable questions and reset their password if they forgot the password. Unlike OAAM, Oracle Identity Manager also has a rich set of password validation capabilities, and it enables policies to be set based on the accounts owned, in addition to simple attributes.

In an Identity and Access Management deployment, best practice is to register only a single set of challenge questions, and to use a single set of password policies. OAAM can be integrated with Oracle Identity Manager so that OAAM provides the challenge questions and Oracle Identity Manager provides password validation, storage and propagation. This enables you to use OAAM fraud prevention at the same time you use Oracle Identity Manager for password validation. When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

This section contains the following topics:

- Section 12.13.5, "Restarting IAMAccessDomain and IAMGovernanceDomain"
- Section 12.13.6, "Validating OAAM - Oracle Identity Manager Integration"
- Section 12.13.7, "Validating Oracle Identity Manager-OAAM Integration"

12.13.1 Configuring Oracle Identity Manager Encryption Keys in CSF

1. Go to Oracle Enterprise Manager Fusion Middleware Control for the domain IAMAccessDomain at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Log in using the WebLogic administrator account, for example `weblogic_idm`.
3. Expand the **WebLogic Domain** icon in the navigation tree in the left pane.
4. Select the IAMAccessDomain, right click, and select the menu option **Security** and then the option **Credentials** in the sub menu.
5. Click **oaam** to select the map and then click **Create Key**.
6. In the pop-up window, ensure **Select Map** is **oaam**.
7. Enter:
   - **Key Name**: `oim.credentials`
   - **Type**: `Password`
   - **UserName**: `xelsysadm`
   - **Password**: Password for `xelsysadm` account, *`COMMON_IDM_PASSWORD`*
8. Click **OK** to save the secret key to the Credential Store Framework.

12.13.2 Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

When you are deploying Oracle Adaptive Access Manager, and Oracle Identity Manager and Oracle Adaptive Access Manager are in separate domains, you must configure cross-domain trust.

Configure cross-domain trust in the domain IAMAccessDomain, as follows:

1. Log in to WebLogic Administration Console in IAMAccessDomain.
2. Click **Lock and Edit**.
3. Click **IAMAccessDomain** in **Domain Structure** and select the **Security** tab.
4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Choose a password to be used to confirm cross domain trust and type it in the **Credential and Confirm Credential** fields.
7. Click **Save**.
8. Click **Activate Changes**.

Configure Cross-Domain Trust in the domain IAMGovernanceDomain, as follows:

1. Log in to WebLogic Administration Console in IAMGovernanceDomain.
2. Click **Lock and Edit**.
3. Click **IAMGovernanceDomain** in **Domain Structure** and select the **Security** tab.

4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Enter the password you entered into the credential fields of the IAMAccessDomain in the **Credential and Confirm Credential** fields.
7. Click **Save**.
8. Click **Activate Changes**.

12.13.3 Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager

Go to the OAAM Administration Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."

Log in using the `oaamadmin` account you created in Section 12.3.2, "Creating OAAM Users and Groups in LDAP.""

Then proceed as follows:

1. In the navigation tree, click **Properties** under the **Environment** heading and then click **Open**. The properties search page is displayed.
2. To set a property value, enter its name in the **Name** field and click **Search**. The current value is shown in the search results window.
3. Click the entry. The **Value** field is displayed. Enter the new value and click **Save**.
4. Set the following properties to enable Oracle Adaptive Access Manager to integrate with Oracle Identity Manager:
   - **`bharosa.uio.default.user.management.provider.classname`**: `com.bharosa.vcrypt.services.OAAMUserMgmtOIM`
   - **`bharosa.uio.default.signon.links.enum.selfregistration.url`**: `ttps://sso.mycompany.com:443/identity/faces/register?&backUrl=https://sso.mycompany.com:443/identity`
   - **`bharosa.uio.default.signon.links.enum.trackregistration.enabled`**: `true`
   - **`bharosa.uio.default.signon.links.enum.selfregistration.enabled`**: `true`
   - **`bharosa.uio.default.signon.links.enum.trackregistration.url`**: `https://sso.mycompany.com:443/identity/faces/trackregistration?&backUrl=https://sso.mycompany.com:443/identity`
   - **`oaam.oim.passwordflow.unlockuser`**: `true`
   - **`oaam.oim.url`**: `t3://oimhost1vhn.mycompany.com:14000,oimhost2vhn.mycompany.com:14000`

12.13.4 Setting Oracle Identity Manager Properties for OAAM

1. Log in to the Oracle Identity Manager System Administration Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **System Configuration** under the **System Management** heading. The System Configuration window opens.

3. Click **Search** in **Search System Properties**.
4. Click each of the properties shown, then select **Edit**. Set the value of each property as shown and click **Save** to save the value.

> **Note:** The property name appears in the **keyword** column.

- `OIM.DisableChallengeQuestions`: `TRUE`
- `OIM.ChangePasswordURL`: `https://sso.mycompany.com:443/oaam_server/oimChangePassword.jsp`
- `OIM.ChallengeQuestionModificationURL`: `https://sso.mycompany.com:443/oaam_server/oimResetChallengeQuestions.jsp`

12.13.5 Restarting IAMAccessDomain and IAMGovernanceDomain

Restart the following Administration servers and managed servers as described in Chapter 15.1, "Starting and Stopping Components."

- WebLogic Administration Servers
- wls_oam1 and wls_oam2
- wls_oim1 and wls_oim2
- wls_oaam1 and wls_oaam2

12.13.6 Validating OAAM - Oracle Identity Manager Integration

Access the test page you created above, for example: http://sso.mycompany.com/oaam_sso.html. You will be presented with the OAAM login page. Click on the links **Registration** or **Track Registration**. If integration is working you will be directed to OIM.

12.13.7 Validating Oracle Identity Manager-OAAM Integration

Validate that Oracle Identity Manager is integrated with OAAM as follows:

Log in to the Oracle Identity Manager Self Service Console as the `xelsysadm` user.

You are prompted to set up challenge questions and OAAM-specific security pictures.

12.14 Changing Domain to Oracle Adaptive Access Manager Protection

If you want to protect certain resources with OAAM, you can do so by adding the OAAM Protected Resources Authentication Policy created in Section 12.12.5.2, "Creating a Resource in Access Manager."

TO use OAAM authentication for everything:

1. Log in to the Access Management Console at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.

5. Click the **Authentication Policies** tab.
6. Click on the policy **Protected HigherLevel Policy**.
7. Change the value of **Authentication Scheme** to `TAPScheme`.
8. Click **Apply**.

12.15 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier as described in Section 15.5.3.6, "Backing Up the Web Tier."
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Back up the Administration Server domain directory as described in Section 15.5.3.4, "Backing Up the WebLogic Domain IAMGovernanceDomain."
4. Back up the directory as described in Section 15.5.3.2, "Backing Up LDAP Directories."

For information about backing up the application tier configuration, see Section 15.5, "Performing Backups and Recoveries."

13

Configuring Server Migration for an Enterprise Deployment

Configuring server migration allows SOA-managed and Oracle Identity Manager-managed servers to be migrated from one host to another, so that if a node hosting one of the servers fails, the service can continue on another node. This chapter describes how to configure server migration for an Identity and Access Management enterprise deployment.

This chapter contains the following steps:

13.1 Overview of Server Migration for an Enterprise Deployment

Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers. The WLS_OIM1 and WLS_SOA1 Managed Server are configured to restart on OIMHOST2 should a failure occur. The WLS_OIM2 and WLS_SOA2 Managed Servers are configured to restart on OIMHOST1 should a failure occur. The WLS_OIM1, WLS_SOA1, WLS_OIM2 and WLS_SOA2 servers listen on specific floating IPs that are failed over by WebLogic Server Migration.

Perform the steps in the following sections configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers.

13.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

In this section, you set up a user and tablespace for the server migration leasing table:

> **Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi data source for database leasing do not need to be re-created, but they must be retargeted to the clusters being configured with server migration.

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the sysdba user and run the following command:

```
create tablespace leasing
logging datafile 'DB_HOME/oradata/orcl/leasing.dbf'
size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `leasing` and assign to it the `leasing` tablespace:

```
create user leasing identified by password;
grant create table to leasing;
grant create session to leasing;
alter user leasing default tablespace leasing;
alter user leasing quota unlimited on leasing;
```

3. Create the `leasing` table using the `leasing.ddl` script:
   a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

```
WL_HOME/server/db/oracle/817
WL_HOME/server/db/oracle/920
```

   b. Connect to the database as the `leasing` user.
   c. Run the leasing.ddl script in SQL*Plus:

```
@Copy_Location/leasing.ddl;
```

   d. Currently, the script does not commit the change. Enter the following, at the SQL*Plus prompt, after the tool completes:

```
commit;
```

13.3 Creating a GridLink Data Source for Leasing Using the Oracle WebLogic Administration Console

In this section, you create a GridLink data source for the leasing table from the Oracle WebLogic Server Administration Console.

To create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
   - **Name**: Enter a logical name for the data source. For example, `leasing`.
   - **JNDI**: Enter a name for JNDI. For example, `jdbc/leasing`.

- **Database Driver**: Select **For the Database Driver, select Oracle's Driver (Thin) for GridLink Connections Versions: 11 and later**.
- Click **Next**.

5. In the Transaction Options page, de-select **Supports Global Transactions**, and click **Next**.
6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.
7. Enter the following connection properties:
   - **Service Name**: Enter the service name of the database (*IGD_SERVICE_NAME*) with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example: `OIMEDG.mycompany.com`
   - **Host Name and Port**: Enter the SCAN address a
     nd port for the RAC database being used. You can identify this address by querying the appropriate parameter in the database using the TCP Protocol:

     ```
     show parameter remote_listener;

     NAME                 TYPE        VALUE

     ------------------------------------------------

     remote_listener     string      IAMDBSCAN.mycompany.com:1521
     ```

     Note:

   - **Database User Name**: leasing
   - **Password**: For example: welcome1
   - **Confirm Password**: Enter the password again and click **Next**.
8. On the Test GridLink Database Connection page, review the connection parameters and click **Test All Listeners**. Here is an example of a successful connection notification:

   ```
   Connection test for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
   LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN.mycompany.com)
   (PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=OIMEDG.mycompany.com))) succeeded.
   ```

   where port 1521 is *DB_LSNR_PORT* and `oimedg.mycompany.com` is *OIM_DB_SERVICE_NAME*.

   Click **Next**.
9. In the ONS Client Configuration page, do the following:
   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.
   - Enter here also the SCAN address for the RAC database and the ONS remote port as reported by the database (example below) and click **ADD**:

     ```
     srvctl config nodeapps -s

     ONS exists: Local port 6100, remote port 6200, EM port 2016
     ```

   - Click **Next**.

Note: For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

```
IAMDBHOST1.mycompany.com (port 6200)
```

and

```
IAMDBHOST2.mycompany.com (port 6200)
```

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for IAMDBSCAN.mycompany.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select **oim_cluster** and **soa_cluster** as the targets, and **All Servers in the cluster**.
12. Click **Finish**.
13. Click **Activate Changes**.

13.4 Editing Node Manager's Properties File

In this section, you edit Node Manager's properties file. This must be done for the Node Managers on the nodes where the servers are running, OIMHOST1 and OIMHOST2.

The `nodemanager.properties` file is located in the following directory:

SHARED_CONFIG_DIR`/nodemanager`

Add the following properties to enable server migration to work properly:

- `Interface:`

  `Interface=bond0`

  This property specifies the interface name for the floating IP. This will be `bond0` in most topologies. If external Oracle HTTP servers are being used, the managed servers will be listening on `bond1`. In that case, the `bond1` interface must be used here.

- `NetMask:`

  `NetMask=255.255.254.0`

  This property specifies the net mask for the interface for the floating IP. The net mask should the same as the net mask on the interface.

- `UseMACBroadcast:`

  `UseMACBroadcast=true`

  This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the `-b` flag in the `arping` command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
StateCheckInterval=500
bond0=*,NetMask=255.255.254.0
UseMACBroadcast=true
```

> **Note:** The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. If not done already, set the `StartScriptEnabled` property in the `nodemanager.properties` file to true. This is required to enable Node Manager to start the managed servers.
2. Start Node Manager on OIMHOST1 and OIMHOST2 by running the `startNodeManager.sh` script, which is located in the *`WL_HOME`*`/server/bin` directory, or use the procedure described in Section 15.1.3.5.1, "Starting Node Manager."

13.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

On Linux, you set environment and superuser privileges for the `wlsifconfig.sh` script:

Ensure that your PATH environment variable includes the files listed in Table 13–1.

Table 13–1 Files Required for the PATH Environment Variable

File	Located in this directory
wlsifconfig.sh	*`IGD_MSERVER_HOME`*`/bin/server_migration`
wlscontrol.sh	*`WL_HOME`*`/common/bin`
nodemanager.domains	*`WL_HOME`*`/common/nodemanager`

Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.

For security reasons, `sudo` should be restricted to the subset of commands required to run the `wlsifconfig.sh` script. For example, perform the following steps to set the environment and superuser privileges for the `wlsifconfig.sh` script.

> **Note:** Ask the system administrator for the appropriate `sudo` and system rights to perform this step.

Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside `/etc/sudoers` granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`.

To grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

13.6 Configuring Server Migration Targets

In this section, you configure server migration targets. Configuring Cluster Migration sets the `DataSourceForAutomaticMigration` property to `true`.

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 15.2, "About Identity and Access Management Console URLs."
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (**oim_cluster**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock and Edit**.
6. In the **Available** field, select the machines to which to allow migration, **OIMHOST1** and **OIMHOST2**, and click the right arrow.
7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
10. Select the server for which you want to configure migration.
11. Click the **Migration** tab.
12. Select **Automatic Server Migration Enabled** and click **Save**.
13. Click **Activate Changes**.
14. Repeat steps 2 through 13 for the SOA cluster.
15. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured, as described in Section 15.1, "Starting and Stopping Components."

13.7 Testing the Server Migration

In this section, you test that server migration is working properly.

The best way to validate server migration is to start Node Manager manually in a console window as described in Section 15.1.3.5.1, "Starting Node Manager."

To test from OIMHOST1:

1. Stop the WLS_OIM1 Managed Server. To do this, run this command:

   ```
   kill -9 pid
   ```

   where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

```
ps -ef | grep WLS_OIM1
```

2. Watch the Node Manager terminal. You should see a message indicating that WLS_OIM1's floating IP has been disabled.
3. Wait for Node Manager to try a second restart of WLS_OIM1. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

To test from OIMHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart WLS_OIM1 on OIMHOST1, Node Manager on OIMHOST2 should prompt that the floating IP for WLS_OIM1 is being brought up and that the server is being restarted in this node.
2. Access the Oracle Identity Manager Console using the Virtual Host Name, for example: `http://OIMHOST1VHN.mycompany.com:14000/identity`.

Follow the previous steps to test server migration for the WLS_OIM2, WLS_SOA1, and WLS_SOA2 Managed Servers.

Table 13–2 shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 13–2 Managed Server Migration

Managed Server	Migrated From	Migrated To
WLS_OIM1	OIMHOST1	OIMHOST2
WLS_OIM2	OIMHOST2	OIMHOST1
WLS_SOA1	OIMHOST1	OIMHOST2
WLS_SOA2	OIMHOST2	OIMHOST1

Verification From the WebLogic Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain at the address listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **IAMGovernanceDomain** on the left pane.
3. Click the **Monitoring** tab and then the **Migration** sub tab.

   The Migration Status table provides information on the status of the migration.

> **Note:** After a server is migrated, to fail it back to its original node/machine, stop the migrated Managed Server from the Oracle WebLogic Administration Console and see that the appropriate Node Manager starts the original Managed Server on the originally assigned machine.

13.8 Backing Up the Server Migration Configuration

Back up the database and the WebLogic domain, as described in Section 15.5.3, "Performing Backups During Installation and Configuration."

14 Scaling Enterprise Deployments

The reference enterprise topology discussed in this guide is highly scalable. It can be scaled up and or scaled out. This chapter explains how to do so.

To scale up the topology, you add a new component instance to a node already running one or more component instances. To scale out the topology, you add new component instances to new nodes.

This chapter contains the following topics:

14.1 Scaling the Topology

The Oracle Identity and Access Management topology described in the guide has three tiers: the Directory Tier, Application Tier and Web Tier. The components in all three tiers of the Oracle Identity and Access Management topology described in this guide can be scaled up or scaled out.

In this release, the Identity and Access Management Deployment tool cannot be used to scale out or scale up components. Scaling up or out is a manual process, as described in this chapter.

You scale up a topology by adding a new server instance to a node that already has one or more server instances running. You scale out a topology by adding new components to new nodes.

14.2 Scaling the LDAP Directory

Scale the LDAP Directory as follows.

14.2.1 Mounting the Middleware Home when Scaling Out

Oracle Binaries are shared among the LDAP hosts. When scaling out, you must mount the shared binary directory onto the new host.To do this, perform the steps in Section 5.7, "Mounting Shared Storage onto the Host."

14.2.2 Scaling Oracle Unified Directory

The binaries for Oracle Unified Directory are located in *IDM_TOP*, which is shared among the LDAPHOSTs. When scaling out Oracle Unified Directory to a new host, ensure that this directory is mounted to the new host. See Section 5.7, "Mounting Shared Storage onto the Host."

The directory tier has two Oracle Unified Directory nodes, LDAPHOST1 and LDAPHOST2, each running an Oracle Unified Directory instance. The Oracle Unified Directory binaries on either node can be used for creating the new Oracle Unified Directory instance.

Proceed as follows:

1. Assemble information, as listed in Section 14.2.2.1, "Assembling Information for Scaling Oracle Unified Directory."
2. If scaling out, mount the shared storage onto the new LDAPHOST.
3. Follow the steps in Section 14.2.2.2, "Configuring an Additional Oracle Unified Directory Instance."
4. Follow the steps in Section 14.2.2.3, "Validating the New Oracle Unified Directory Instance."
5. Follow the steps in Section 14.2.2.4, "Adding the New Oracle Unified Directory Instance to the Load Balancers."
6. Reconfigure the load balancer with the host and port information of the new Oracle Unified Directory instance, as described in Section 14.4.5, "Reconfiguring the Load Balancer."

14.2.2.1 Assembling Information for Scaling Oracle Unified Directory

Assemble the following information before scaling Oracle Unified Directory.

Description	Variable	Documented Value	Customer Value
New Oracle Unified Directory Host Name	*LDAP_HOST*	LDAPHOST3.mycompany.com	
Oracle Unified Directory Listen Port	*LDAP_PORT*	1389	
Oracle Unified Directory SSL Port	*LDAP_SSL_PORT*	1636	
Oracle Unified Directory Administration Port	*LDAP_ADMIN_PORT*	4444	
Oracle Unified Directory Replication Port	*LDAP_REPLIC_PORT*	8989	
Oracle Instance Location	*OUD_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oud*n*	
Oracle Unified Directory Existing Instance/Component Name	oud*n*	oud1	
Newly Created Instance/Component Name	oud*n*	oud3	
Oracle Unified Directory Administrator Password	*COMMON_IDM_PASSWORD*		
Common Password	*COMMON_IDM_PASSWORD*		

14.2.2.2 Configuring an Additional Oracle Unified Directory Instance

If you are scaling out to another machine, you can use ports 1389 (*LDAP_PORT*), 1636 *(LDAP_SSL_PORT*), 4444 (*LDAP_ADMIN_PORT*), and 8989. If you are scaling up, those ports are already in use and you must choose unique ports. Ensure that the ports you plan to use are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

```
netstat -an | grep "1389"
```

If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

Remove the entries for the ports you freed from the `/etc/services` file and restart the services or restart the computer.

Set the environment variable `JAVA_HOME`

Set the environment variable `INSTANCE_NAME` to a new instance value, such as: `../../../../u02/private/oracle/config/instances/oud3`

Note the tool creates the instance home relative to the *`OUD_ORACLE_HOME`*, so you must include previous directories to get the instance created in *`OUD_ORACLE_INSTANCE`*.

Change Directory to *`OUD_ORACLE_HOME`*

Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

1. On the Welcome screen, click **Next**.
2. On the Server Settings screen, enter:
   - **Host Name**: The name of the host where Oracle Unified Directory is running, for example: LDAPHOST3
   - **LDAP Listener Port**: 1389 (*LDAP_PORT*) if scaling out, unique port if scaling up.
   - **Administration Connector Port**: 4444 (*LDAP_ADMIN_PORT*)
   - LDAP Secure Access
     - Click **Configure**
     - Select **SSL Access**
     - **Enable SSL on Port**: 1636 *(LDAP_SSL_PORT*)
     - **Certificate**: Generate Self Signed Certificate OR provide details of your own certificate.
     - Click **OK**
   - **Root User DN**: Enter an administrative user for example `cn=oudadmin`
   - **Password**: Enter the password you want to assign to the ouadmin user. Using the *`COMMON_IDM_PASSWORD`* is recommended.
   - **Password (Confirm)**: Repeat the password.
   - Click **Next**.
3. On the Topology Options screen, enter
   - **This server will be part of a replication topology**

- **Replication Port:** (*LDAP_REPLIC_PORT*) 8989
- Select **Configure As Secure,** if you want replication traffic to be encrypted.
- **There is already a server in the topology**: Selected.

  Enter the following:

  – **Host Name**: The name of the Oracle Unified Directory server host for this instance, for example: LDAPHOST1.mycompany.com

  – **Administrator Connector Port**: 4444 (*LDAP_ADMIN_PORT*)

  – **Admin User**: Name of the Oracle Unified Directory administrative user on LDAPHOST1, for example: `cn=oudadmin`

  – **Admin Password**: Administrator password. Using the *COMMON_IDM_PASSWORD* is recommended.

  Click **Next**.

  If you see a certificate Not Trusted Dialogue, it is because you are using self signed certificates. Click **Accept Permanently.**

Click **Next**.

4. On The Create Global Administrator Screen Enter:
   - **Global Administrator ID:** The name of an account you want to use for managing Oracle Unified Directory replication, for example: `oudmanager`
   - **Global Administrator Password / Confirmation**: Enter a password for this account. Using the *COMMON_IDM_PASSWORD* is recommended.

   Click **Next**.
5. On the Data Replication Screen. select `dc=mycompany,dc=com` and click **Next**.
6. On the Oracle Components Integration screen, click **Next**.
7. On the Runtime Options Screen Click Next.
8. On the Review Screen, check that the information displayed is correct and click **Finish**.
9. On the Finished screen, click **Close**.

14.2.2.3 Validating the New Oracle Unified Directory Instance

After configuration, you can validate that Oracle Unified Directory is working by performing a simple search. To do this issue the following command:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAPHOST3.mycompany.com -p 1389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl
```

If Oracle Unified Directory is working correctly, you will see a list `supportedControl` entries returned.

14.2.2.4 Adding the New Oracle Unified Directory Instance to the Load Balancers

Add the new Oracle Unified Directory instance to the existing server pool defined on the load balancer for distributing requests across the instances.

14.3 Scaling Identity and Access Management Applications

The Application Tier has two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Access Management Access Manager, and two nodes (OIMHOST1 and OIMHOST2) running Managed Servers for Oracle Identity Manager. Optionally, the Application Tier might have two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Adaptive Access Manager.

This section contains the following topics:

14.3.1 Gathering Information

Use the following tables to assemble the values you need.

14.3.1.1 Assembling Information for Scaling Access Manager

Assemble the following information before scaling Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	NEWHOST*n*		
Existing Access Manager server		WLS_OAM1	
New Access Manager server name	WLS_OAM*n*	WLS_OAM3	
Server Listen Port	*OAM_PORT*	14100	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IADADMINVHN.mycompany.com	
WebLogic Administration Port	*IAD_WLS_PORT*	7001	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

14.3.1.2 Assembling Information for Scaling Oracle Identity Manager

Description	Variable	Documented Value	Customer Value
Host name	NEWHOST*n*		
SOA virtual server name		SOAHOST*x*VHN	
Oracle Identity Manager virtual server name		OIMHOST*x*VHN	
Existing SOA managed server to clone	WLS_SOA*n*	WLS_SOA1	

Description	Variable	Documented Value	Customer Value
Existing Oracle Identity Manager managed server to clone	WLS_OIM*n*	WLS_OIM1	
New SOA managed server name	WLS_SOA*n*	WLS_SOA3	
New Oracle Identity Manager managed server name	WLS_OIM*n*	WLS_OIM3	
Numeric extension for new JMS servers	*n*	3	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IGDADMINVHN.mycompany.com	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7101	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

14.3.1.3 Assembling Information for Scaling Oracle Adaptive Access Manager

Assemble the following information before scaling Oracle Adaptive Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	*NEWHOSTn*		
Existing OAAM server		WLS_OAAM1	
New OAAM server name	*WLS_OAAMn*	WLS_OAAM3	
Server Listen Address			
OAAM Managed Server Port	*OAAM_PORT*	14200	
OAAM Administration Managed Server Port	*OAAM_ADMIN_PORT*	14300	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IADADMINVHN.mycompany.com[1]	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7001	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

[1] This refers to the domain that you are scaling.

14.3.2 Mounting Middleware Home and Creating a New Machine when Scaling Out

Before scaling out a component of the OAM application tier, mount the Middleware home and create a new machine.

To mount the Middleware home and create a new machine:

1. On the new node, mount the existing Middleware home, which should include the Oracle Fusion Middleware installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain. See Section 5.7, "Mounting Shared Storage onto the Host." for more information.
2. To attach *IAD_ORACLE_HOME* in shared storage to the local Oracle Inventory, execute the following command:

```
cd IAD_ORACLE_HOME/oui/bin
./attachHome.sh -jreLoc JAVA_HOME
```

Note: This section uses IAD_ORACLE_HOME as an example. Use the same procedure for IGD_ORACLE_HOME.

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *HOME*/bea/beahomelist file and add *IAD_MW_HOME*/oui/bin to it.
4. Log in to the WebLogic Administration Console for the IAMAccessDomain at the address listed in Section 15.2, "About Identity and Access Management Console URLs."
5. Create a new machine for the new node to be used, and add the machine to the domain, as follows.
   a. Select **Environment -> Machines** from the Navigation menu.
   b. Click **Lock and Edit**.
   c. Click **New** on the Machine Summary screen.
   d. Enter the following information:

      Name: Name of the machine (NEWHOSTn)

      Machine OS: Select UNIX.
   e. Click **Next**.
   f. On the Node Manager Properties page, enter the following information:

      Type: SSL.

      Listen Address: *NEWHOSTn*.
   g. Click **Finish**.
   h. Click **Activate Changes**.

14.3.3 Creating a New Node Manager when Scaling Out

Node Manager is used to start and stop WebLogic managed servers on the new host. In order to create a new node manager for the new host perform the following steps:

1. Create a new directory for the new node manager by copying an existing one. Copy the directory *SHARED_CONFIG*/nodemanager/oamhost1.mycompany.com to: *SHARED_CONFIG*/nodemanager/*newiamhost*.mycompany.com

   For example:

   ```
   cp -r $SHARED_CONFIG/nodemanager/oamhost1.mycompany.com $SHARED_
   CONFIG/nodemanager/newiamhost.mycompany.com
   ```

2. Change to the newly created directory.

   ```
   cd SHARED_CONFIG/nodemanager/NEWHOST3.mycompany.com
   ```

3. Edit the nodemanager.properties file, changing all the entries for OAMHOST1 to OAMHOST3. For example:

   ```
   DomainsFile=/u01/oracle/config/nodemanager/OAMHOST1.mycompany.com/nodemanager.d
   ```

```
omain
```

becomes

```
DomainsFile=/u01/oracle/config/nodemanager/NEWHOST3.mycompany.com/nodemanager.d
omain
```

4. Edit the `startNodeManagerWrapper.sh` file, changing all the entries for OAMHOST1 to OAMHOST3. For example:

```
NM_HOME=/u01/oracle/config/nodemanager/oamhost1.mycompany.com
```

becomes

```
NM_HOME=/u01/oracle/config/nodemanager/oamhost3.mycompany.com
```

5. Start the node manager by invoking the command:

```
./startNodeManagerWrapper.sh
```

6. Update the node manager configuration by following the steps in Chapter 14.5.3, "Updating Node Manager Configuration" to ensure that certificates are created for the new host.

14.3.4 Running Pack/Unpack

Whenever you extend a domain to include a new managed server, you must extract the domain configuration needs from the *ASERVER_HOME* location to the *MSERVER_HOME* location. This applies whether you are scaling up or out. To do this perform the following steps.

> **Note:** The following steps are an example of packing and unpacking the IAMAccessDomain

1. Pack the domain on the host where the administration server is located, for example: OAMHOST1:

```
pack.sh -domain=IAD_ASERVER_HOME -template =/templates/managedServer.jar
-template_name="template_name" -managed=true
```

The `pack.sh` script is located in *ORACLE_COMMON_HOME*`/common/bin`.

2. Unpack the domain on the new host for scale out, or on the existing host for scale up, using the command:

```
unpack.sh -domain=IAD_MSERVER_HOME -template=/templates/managedServer.jar -app_
dir=IAD_MSERVER_HOME/applications
```

The `unpack.sh` script is located in *ORACLE_COMMON_HOME*`/common/bin`.

3. If you are scaling out, start Node Manager and update the property file.
   a. Start and stop Node Manager as described in Section 15.1, "Starting and Stopping Components."
   b. Run the script `setNMProps.sh`, which is located in *ORACLE_COMMON_HOME*`/common/bin`, to update the node manager properties file, for example:

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

c. Start Node Manager once again as described in Section 15.1, "Starting and Stopping Components."

14.3.5 Performing Application-Specific Steps

This section contains the following topics:

- Section 14.3.5.1, "Clone an Existing Managed Server."
- Section 14.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 14.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 14.3.5.3, "Scaling Oracle Identity Manager"
- Section 14.3.5.4, "Updating Oracle Adaptive Access Manager Integration"

14.3.5.1 Clone an Existing Managed Server

Create a new managed server by cloning an existing managed server of the same type. To scale out/up Access Manager, clone `wls_oam1`. Similarly, to scale out/up Identity Manager, clone `wls_oim1`.

The following example is for cloning an Access Manager managed server, although the procedure is the same for all products.

1. Log in to the Oracle WebLogic Administration Console for the domain whose managed server you are cloning, at the address listed in Section 15.2, "About Identity and Access Management Console URLs." For this example the domain is `IAMAccessDomain`.
2. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
3. Click **Lock & Edit** from the Change Center menu.
4. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.
5. Click **Clone**.
6. Enter the following information:
   - **Server Name**: A new name for the server, for example: `WLS_OAM3`.
   - **Server Listen Address**: The name of the host on which the Managed Server runs.
   - **Server Listen Port**: The port the new Managed Server uses. This port must be unique within the host.

     If you are scaling out, you can use the default port, `14100` (*`OAM_PORT`* in Table 7–1). If you are scaling up, choose a unique port.
7. Click **OK**.
8. Click the newly created server **WLS_OAM3**
9. Set **Machine** to be the machine you created in Section 14.3.2, "Mounting Middleware Home and Creating a New Machine when Scaling Out""
10. Click **Save**.
11. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_OAM3` Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the

communication between the Oracle WebLogic Administration Server and the Node Manager in `NEWHOST`.

If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings were propagated to the cloned server. To disable host name verification:

a. In Oracle Enterprise Manager Fusion Middleware Control, select **Oracle WebLogic Server Administration Console**.

b. Expand the **Environment** node in the Domain Structure window.

c. Click **Servers**. The Summary of Servers page appears.

d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.

e. Click the **SSL** tab.

f. Click **Advanced**.

g. Set **Hostname Verification** to `None`.

h. Click **Save**.

12. Click **Activate Changes** from the Change Center menu.

14.3.5.2 Scaling Oracle Access Management Access Manager

This section contains steps specific to scaling Access Manager.

Note: If you are using shared storage, allow the new host access to that shared storage area.

Scale Oracle Access Management Access Manager by performing the steps in the following subsections:

- Section 14.3.5.2.1, "Run Pack/Unpack"
- Section 14.3.5.2.2, "Register Managed Server with Oracle Access Management Access Manager"
- Section 14.3.5.2.3, "Update WebGate Profiles"
- Section 14.3.5.2.4, "Update the Web Tier"

14.3.5.2.1 Run Pack/Unpack Run `pack` and `unpack` as described in Section 15.3.4, "Running Pack/Unpack."

14.3.5.2.2 Register Managed Server with Oracle Access Management Access Manager Register the new Managed Server with Oracle Access Management Access Manager. You now must configure the new Managed Server now as an Access Manager server. You do this from the Oracle Access Management Console. Proceed as follows:

1. Log in to the Access Management console at `http://IADADMIN.mycompany.com/oamconsole` as the user identified by the entry in Section 8.9, "Set User Names and Passwords"
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.

5. Enter the following information:
   - **Server Name**: `WLS_OAM3`
   - **Host**: Host that the server runs on
   - **Port**: Listen port that was assigned when the Managed Server was created
   - **OAM Proxy Port**: Port you want the Access Manager proxy to run on. This is unique for the host
   - **Proxy Server ID**: `AccessServerConfigProxy`
   - **Mode**: Set to same mode as existing Access Manager servers.
6. Click **Coherence** tab.

   Set **Local Port** to a unique value on the host.
7. Click **Apply**.
8. Restart the WebLogic Administration Server as described in Section 15.1, "Starting and Stopping Components"

14.3.5.2.3 Update WebGate Profiles Add the newly created Access Manager server to all WebGate Profiles that might be using it, such as `Webgate_IDM`, `Webgate_IDM_11g`, and `IAMSuiteAgent`

For example, to add the Access Manager server to `Webgate_IDM`, access the Access Management console at: `http://IADADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Log in as the Access Manager Administrative User.
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings** - **SSO Agents** - **OAM Agents**.
4. Click the open folder icon, then click **Search**.

   You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.
7. Click **+** in the **Primary Server** list (or the **Secondary Server** list if this is a secondary server).
8. Select the newly created managed server from the **Server** list.
9. Set **Maximum Number of Connections** to `10`.
10. Click **Apply**.

Repeat Steps 5 through 10 for **Webgate_IDM_11g**, **IAMSuiteAgent**, and all other WebGates that might be in use.

You can now start the new Managed Server, as described in Section 15.1, "Starting and Stopping Components"

14.3.5.2.4 Update the Web Tier Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 14.3.6, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files"

Save the file and restart the Oracle HTTP server, as described in Section 15.1, "Starting and Stopping Components"

14.3.5.3 Scaling Oracle Identity Manager

You already have a node that runs a Managed Server configured with Oracle SOA Suite and Oracle Identity Manager components. The node contains a Middleware home, a SOA Oracle home, an Oracle Identity Manager Oracle home, and a domain directory for existing Managed Servers. Use the existing installations in shared storage for creating a new WLS_SOA and WLS_OIM managed server. There is no need to install the Oracle Identity and Access Management or Oracle SOA Suite binaries in a new location

When scaling up, you add WLS_SOA and WLS_OIM managed servers to existing nodes.

In either case, you must run pack and unpack.

When you scale out the topology, you add new Managed Servers configured with Oracle Identity Manager and SOA to new nodes. First check that the new node can access the existing home directories for WebLogic Server, Oracle Identity Manager, and SOA. You do need to run pack and unpack to bootstrap the domain configuration in the new node.

Follow the steps in the following subsections to scale the topology:

- Section 14.3.5.3.1, "Configuring New JMS Servers"
- Section 14.3.5.3.2, "Performing Pack/Unpack When Scaling Out"
- Section 14.3.5.3.3, "Configuring Oracle Coherence for Deploying Composites"
- Section 14.3.5.3.4, "Enabling Communication for Deployment Using Unicast Communication"
- Section 14.3.5.3.5, "Specifying the Host Name Used by Oracle Coherence"
- Section 14.3.5.3.6, "Completing the Oracle Identity Manager Configuration Steps"

14.3.5.3.1 Configuring New JMS Servers Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server. You do this as follows:

1. Log in to the WebLogic Administration Server in the IAMGovernanceDomain, as described in Section 15.2, "About Identity and Access Management Console URLs," and navigate to **Services -> Messaging -> JMS Servers**.
2. Click **New**.
3. Enter a value for **Name**, such as `BPMJMSServer_auto_3`.
4. Click **Create New Store**.
5. Select `FileStore` from the list
6. Click **Next**.
7. Enter a value for **Name**, such as `BPMJMSFileStore_auto_3`
8. Enter the following values:

   Target: The new server you are creating.

   Directory: *`IGD_ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_3`
9. Click **OK**.
10. When you are returned to the JMS Server screen, select the newly created file store from the list.
11. Click **Next**.

12. On the next screen set the Target to the server you are creating.
13. Click **Finish**.

Create the following JMS Queues depending on the managed server you are creating:

Server	JMS Server Name	File Store Name	Directory	Target
WLS_SOA*n*	BPMJMSServer_auto_*n*	BPMJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/BPMJMSFileStore_auto_*n*	WLS_SOA*n*
WLS_SOA*n*	SOAJMSServer_auto_*n*	SOAJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/SOAJMSFileStore_auto_*n*	WLS_SOA*n*
WLS_SOA*n*	UMSJMSServer_auto_*n*	UMSJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/UMSJMSFileStore_auto_*n*	WLS_SOA*n*
WLS_OIM*n*	JRFWSAsyncJmsServer_auto_*n*	JRFWSAsyncFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/RFWSAsyncFileStore_auto_*n*	WLS_OIM*n*
WLS_OIM*n*	OIMJMSServer_auto_*n*	OIMJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/OIMJMSFileStore_auto_*n*	wls_OIM*n*
WLS_SOA*n*	PS6SOAJMSServer_auto_*n*	PS6SOAJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*/jms/PS6SOAJMSFileStore_auto_*n*	wls_SOA*n*

Add the newly created JMS Queues to the existing JMS Modules by performing the following steps:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain, at the address listed in Section 15.2, "About Identity and Access Management Console URLs."
2. Navigate to **Services -> Messaging -> JMS Modules**
3. Click a JMSModule, such as **SOAJMSModule**
4. Click the **Sub Deployments** tab.
5. Click the listed sub deployment.

> **Note:** This subdeployment module name is a random name in the form of **JMSServerName*XXXXXX*** resulting from the Configuration Wizard JMS configuration.

6. Assign the newly created JMS server, for example **SOAJMSServer_auto*n***.
7. Click **Save**.
8. Perform this for each of the JMS modules listed in the following table:

JMS Module	JMS Server
BPMJMSModule	BPMJMSServer_auto_*n*
JRFWSAsyncJmsModule	JRFWSAsyncJmServer_auto_*n*
OIMJMSModule	OIMJMSServer_auto_*n*

JMS Module	JMS Server
SOAJMSModule	SOAJMSServer_auto_*n*
UMSJMSSystemResource	UMSJMSServe_auto_*n*

9. Click **Activate Configuration** from the Change Center menu.

14.3.5.3.2 Performing Pack/Unpack When Scaling Out This section is necessary only when you are scaling out.

Run `pack` and `unpack` as described in Section 14.3.4, "Running Pack/Unpack"

14.3.5.3.3 Configuring Oracle Coherence for Deploying Composites Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Note:** An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

14.3.5.3.4 Enabling Communication for Deployment Using Unicast Communication Specify the nodes using the `tangosol.coherence.wkan` system property, where *n* is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses, for example: SOAHOST3VHN. Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab. You will also need to add the new server to the existing entries.

> **Tip:** To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

> **Note:** SOAHOST3VHN is the virtual host name that maps to the virtual IP where WLS_SOA3 listening (in SOAHOST3).

14.3.5.3.5 Specifying the Host Name Used by Oracle Coherence Use the Administration Console to specify a host name used by Oracle Coherence.

To add the host name used by Oracle Coherence:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (**WLS_SOA1** or **WLS_SOA2**, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Enter the following for WLS_SOA1, WLS_SOA2, and WLS_SOA3 into the Arguments field.

   For WLS_SOA1, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST1VHN
   ```

   For WLS_SOA2, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST2VHN
   ```

   For WLS_SOA3, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST3VHN
   ```

   Note: There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the text to your Administration Console's arguments text field. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST1VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST2VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA3 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST3VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

For more information about Coherence Clusters see the *Oracle Coherence Developer's Guide*.

8. Click **Save** and **Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

14.3.5.3.6 Completing the Oracle Identity Manager Configuration Steps

1. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

   From the WebLogic Administration Console, select the **Server_name** > **Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

2. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOA`*n* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `OIMHOST`*n*. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

   To disable host name verification:

   a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.

   b. Expand the **Environment** node in the Domain Structure window.

   c. Click **Servers**. The Summary of Servers page appears.

   d. Select **WLS_SOA*n*** in the Names column of the table. The Settings page for the server appears.

   e. Click the **SSL** tab.

   f. Click **Advanced**.

   g. Set **Hostname Verification** to `None`.

   h. Click **Save**.

3. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIM`*n* Managed Servers. In Step d, select **WLS_OIM*n*** in the Names column of the table.

4. Click **Activate Changes** from the Change Center menu.

5. Restart the WebLogic Administration Server as described in Section 15.1, "Starting and Stopping Components"

6. Start and test the new Managed Server from the Administration Console.

   a. Shut down the existing Managed Servers in the cluster.

   b. Ensure that the newly created Managed Server, `WLS_SOA`*n*, is up.

   c. Access the application on the newly created Managed Server (`http://vip:port/soa-infra`). The application should be functional.

7. Configure the newly created managed server for server migration. Follow the steps in Section 13.6, "Configuring Server Migration Targets"to configure server migration.

Note: Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP addresses for the new Managed Servers are already present in the new node.

8. Test server migration for this new server. Follow these steps from the node where you added the new server:
   a. Stop the `WLS_SOA`*n* Managed Server.

      To do this, run:

      ```
      kill -9 pid
      ```

      on the process ID (PID) of the Managed Server. You can identify the PID of the node using

      ```
      ps -ef | grep WLS_SOAn
      ```

   b. Watch the Node Manager Console. You should see a message indicating that the floating IP address for WLS_SOA1 has been disabled.
   c. Wait for the Node Manager to try a second restart of WLS_SOA*n*. Node Manager waits for a fence period of 30 seconds before trying this restart.
   d. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.
   e. Repeat Steps a-d for WLS_OIM*n*.

14.3.5.4 Updating Oracle Adaptive Access Manager Integration

If you have extended your domain with Oracle Adaptive Access Manager and have integrated Oracle Identity Manager with Oracle Adaptive Access Manager, you must update Oracle Adaptive Access Manager so that it is aware of the new Oracle Identity Manager server. See Section 12.13.3, "Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager" for details.

14.3.6 Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files

Scaling an Application Tier component typically requires you to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

In the Web tier, there are several configuration files under *`WEB_ORACLE_INSTANCE`*`/config/OHS/componentname/moduleconf`, including `admin_vh.conf`, `sso_vh.conf` and `idminternal_vh.conf`. Each contain a number of entries in location blocks. If a block references two server instances and you add a third one, you must update that block with the new server.

For example if you add a new Access Manager server, you must update `sso_vh.conf` to include the new managed server. You add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100,OAMHOST1.mycompany.com:1
4101
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100,OAMHOST3.mycompany.com:1
4100
</Location>
```

Once you have updated the configuration file, restart the Oracle HTTP server(s) as described in Section 15.1, "Starting and Stopping Components." Oracle recommends that you do this sequentially to prevent loss of service.

14.4 Scaling the Web Tier

The Web Tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance.

To scale the Oracle HTTP Server, perform the steps in the following subsections:

- Section 14.4.1, "Assembling Information for Scaling the Web Tier."
- Section 14.4.2, "Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out."
- Section 14.4.3, "Running the Configuration Wizard to Configure the HTTP Server."
- Section 14.4.4, "Registering Oracle HTTP Server with WebLogic Server."
- Section 14.4.5, "Reconfiguring the Load Balancer."

14.4.1 Assembling Information for Scaling the Web Tier

Assemble the following information before scaling the Web Tier.

Description	Variable	Documented Value	Customer Value
Host name		WEBHOST1.mycompany.com	
OHS port	*WEB_HTTP_PORT*	7777	
Instance Name	web*n*	web1 or web2	
Component Name	web*n*	web1 or web2	

Description	Variable	Documented Value	Customer Value
WebLogic Administration Host, IAMAccessDomain	*IADADMINVHN*	IADADMINVHN.mycompany.com	
Access Management WLS Server Port	*IAD_WLS_PORT*	7001	
WebLogic Administrative User		weblogic_idm	
WebLogic Administrative Password			

14.4.2 Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out

On the new node, mount the existing Middleware home.

Copy all files created in *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf from the existing Web Tier configuration to the new one.

14.4.3 Running the Configuration Wizard to Configure the HTTP Server

Perform these steps to configure the Oracle Web Tier:

1. Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the file stage/Response/staticports.ini. Copy it to a file called ohs_ports.ini. Delete all entries in ohs_ports.ini except for OHS PORT and OPMN Local Port. Change the value of OPMN Local Port to 6700. If you are scaling out, you can use the default value, 7777, for OHS PORT. If you are scaling up, you must choose a unique value for that instance on the machine.

   Note: If the port names in the file are slightly different from OHS PORT and OPMN Local Port, use the names in the file.

2. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

   ```
   cd WEB_ORACLE_HOME/bin
   ```

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

   Ensure that Associate Selected Components with WebLogic Domain is selected.

   Ensure Oracle Web Cache is **NOT** selected.

   Click **Next**.
3. On the Specify WebLogic Domain Screen, enter
   - **Domain Host Name**: IADADMINVHN.mycompany.com
   - **Domain Port No**: 7001, where 7001 is *IAD_WLS_PORT* in Section 7.1, "Assembling Information for Identity and Access Management Deployment."

- **User Name**: Weblogic Administrator User (For example: `weblogic`)
- **Password**: Password for the Weblogic Administrator User account

Click **Next**.

4. On the Specify Component Details screen, specify the following values:

   Enter the following values for WEBHOST*n*, where *n* is the number of the new host, for example, `3`:

   - **Instance Home Location**: *`WEB_ORACLE_INSTANCE`*, for example: `/u02/local/oracle/config/instances/ohs1`
   - **Instance Name**: `webn`
   - **OHS Component Name**: `webn`

   Click **Next**.

5. On the Configure Ports screen, you use the `ohs_ports.ini` file you created in Step 1to specify the ports to be used. This enables you to bypass automatic port configuration.

   a. Select **Specify Ports using a Configuration File**.

   b. In the file name field specify `ohs_ports.ini`.

   c. Click **Save**, then click **Next**.

6. On the Specify Security Updates screen, specify these values:

   - **Email Address**: The email address for your My Oracle Support account.
   - **Oracle Support Password**: The password for your My Oracle Support account.

   Select: **I wish to receive security updates via My Oracle Support**.

   Click **Next**.

7. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

   Click **Configure**.

   On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

   On the Installation Complete screen, click **Finish** to confirm your choice to exit.

14.4.4 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the new Oracle HTTP server, you must register the Oracle HTTP server with IAMAccessDomain. To do this, register Oracle HTTP Server with WebLogic Server by running the following command on the host where the new server is running:

```
cd WEB_ORACLE_INSTANCE/bin
./opmnctl registerinstance -adminHost IADADMINVHN.mycompany.com \
   -adminPort WLS_ADMIN_PORT -adminUsername weblogic
```

14.4.5 Reconfiguring the Load Balancer

Add the new Oracle HTTP Server instance to the existing server pool defined on the load balancer for distributing requests across the HTTP instances.

14.5 Post-Scaling Steps for All Components

Perform the following post-scaling steps.

- Section 14.5.1, "Updating the Topology Store."
- Section 14.5.2, "Updating Stop/Start Scripts."
- Section 14.5.3, "Updating Node Manager Configuration."

14.5.1 Updating the Topology Store

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Lifecycle Tools read the store in order to build and execute the patch plan. If you scale out/up the topology you must add new entries to the store covering the new additions to the deployment.

To do this follow the steps in Appendix C, "Topology Tool Commands for Scaling."

14.5.2 Updating Stop/Start Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. When you create a new managed server in the domain you need to update the domain configuration so that these start and stop scripts can also start the newly created managed server.

To update the domain configuration, edit the file `serverInstancesCustom.txt`, which is located in the directory: *`SHARED_CONFIG`*`/scripts`

14.5.3 Updating Node Manager Configuration

Update the node manager configuration, as described in the following sections:

- Section 14.5.3.1, "Starting and Stopping Node Manager."
- Section 14.5.3.2, "Setting Up Node Manager for an Enterprise Deployment."

14.5.3.1 Starting and Stopping Node Manager

If you want to start a node manager on a new machine, add an entry which looks like this:

`newmachine``.mycompany.com NM` *`nodemanager_pathname nodemanager_port`*

For example:

```
OAMHOST3.mycompany.com NM /u01/oracle/config/nodemanager/oamhost3.mycompany.com
5556
```

If you want to start a managed server called WLS_OIM3 add an entry which looks like this:

`newmachine``.mycompany.com OIM` *`ManagedServerName`*

For example:

```
OAMHOST3 OIM WLS_OIM3
```

Save the file.

If you added a new node manager, you must enable it for SSL as described in Section 14.5.3.2, "Setting Up Node Manager for an Enterprise Deployment."

14.5.3.2 Setting Up Node Manager for an Enterprise Deployment

This section describes how to configure Node Manager in accordance with Oracle best practice recommendations. It contains the following subsections:

- Section 14.5.3.2.1, "Enabling Host Name Verification Certificates for Node Manager."
- Section 14.5.3.2.2, "Generating Self-Signed Certificates Using the utils.CertGen Utility."
- Section 14.5.3.2.3, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."
- Section 14.5.3.2.4, "Creating a Trust Keystore Using the Keytool Utility."
- Section 14.5.3.2.5, "Configuring Node Manager to Use the Custom Keystores."
- Section 14.5.3.2.6, "Configuring Managed WebLogic Servers to Use the Custom Keystores."
- Section 14.5.3.2.7, "Changing the Host Name Verification Setting for the Managed Servers."
- Section 14.5.3.2.8, "Starting Node Manager."

14.5.3.2.1 Enabling Host Name Verification Certificates for Node Manager This section describes how to set up host name verification certificates for communication between Node Manager and the Administration Server.

14.5.3.2.2 Generating Self-Signed Certificates Using the utils.CertGen Utility The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST*.mycompany.com) and a WebLogic Managed Server listens on a virtual host name (*VIP*.mycompany.com). Whenever a server is using a virtual host name, it is implied that the server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example must be extended to:

1. Add the required host names to the certificate stores (if they are different from *HOST*.mycompany.com and *VIP*.mycompany.com).
2. Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by Managed Servers).

Follow these steps to create self-signed certificates on *HOST*. These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*. The following examples configure certificates for *HOST*.mycompany.com and *VIP*.mycompany.com; that is, it is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST*.mycompany.com is the address used by Node Manager and *VIP*.mycompany.com is the address used by a Managed Server or the Administration Server. This is the common situation for nodes hosting an Administration Server and a Fusion Middleware component, or for nodes where two Managed Servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the *WL_HOME*/server/bin/setWLSEnv.sh script. In the Bourne shell, run the following commands:

```
cd WL_HOME/server/bin
. ./setWLSEnv.sh
```

Verify that the *CLASSPATH* environment variable is set:

```
echo $CLASSPATH
```

2. Create a user-defined directory for the certificates. For example, create a directory called 'keystores' under the *ASERVER_HOME* directory. Note that certificates can be shared across WebLogic domains.

```
cd SHARED_CONFIG
mkdir keystores
```

> **Note:** The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, for example).

3. Change directory to the directory that you just created:

```
cd keystores
```

4. Using the `utils.CerGen` tool, create certificates for each Physical and Virtual Host in the topology.

Syntax (all on a single line):

```
java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
[export | domestic] [Host_Name]
```

Examples are:

```
java utils.CertGen Key_Passphrase NEWHOST.mycompany.com_cert
NEWHOST.mycompany.com_key domestic NEWHOST.mycompany.com
```

Also create certificates for any new virtual hosts.

```
java utils.CertGen Key_Passphrase NEWVHN.mycompany.com_cert
NEWVHN.mycompany.com_key domestic NEWVHN.mycompany.com
```

14.5.3.2.3 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

Follow these steps when adding a new host:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, *ASERVER_HOME*`/keystores`).

> **Note:** The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store using the `utils.ImportPrivateKey` utility.

2. Import the certificate and private key for each of the certificates created above into the Identity Store. Ensure that you use a different alias for each of the certificate/key pairs imported.

   Syntax (all on a single line):

   ```
   java utils.ImportPrivateKey Keystore_File Keystore_Password
   Certificate_Alias_to_Use Private_Key_Passphrase
   Certificate_File
   Private_Key_File
   [Keystore_Type]
   ```

   Examples:

   ```
   java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
   appIdentityNEWHOST Key_Passphrase SHARED_
   CONFIG/keystores/NEWHOST.mycompany.com_cert.pem SHARED_
   CONFIG/keystores/NEWHOST.mycompany.com_key.pem
   ```

14.5.3.2.4 Creating a Trust Keystore Using the Keytool Utility Follow these steps to create a new Keystore for each new host.

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the *WL_HOME*/server/lib directory to the same directory as the certificates. For example:

   ```
   cp WL_HOME/server/lib/cacerts SHARED_
   CONFIG/keystores/appTrustKeyStoreNEWHOST.jks
   ```

2. The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password. Use the `keytool` utility to do this. The syntax is:

   ```
   keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
   Original_Password
   ```

   For example:

   ```
   keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStoreNEWHOST.jks
   -storepass changeit
   ```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *WL_HOME*/server/lib directory. This CA certificate must be imported into the `appTrustKeyStore` using the `keytool` utility. The syntax is:

   ```
   keytool -import -v -noprompt -trustcacerts -alias Alias_Name
   -file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
   ```

   For example:

   ```
   keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_
   HOME/server/lib/CertGenCA.der -keystore appTrustKeyStoreNEWHOST.jks -storepass
   Key_Passphrase
   ```

14.5.3.2.5 Configuring Node Manager to Use the Custom Keystores After adding a new node manager you need to configure it to use the new custom keystones described in Section 14.5.3.2.4, "Creating a Trust Keystore Using the Keytool Utility.". To configure

Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` file located in the *SHARED_CONFIG*`/nodemanager/`*hostname* directory, where *hostname* is the name of the host where nodemanager runs:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=SHARED_CONFIG/keystores/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentityNEWHOST
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the `nodemanager.properties` file get encrypted when you start Node Manager as described in Section 15.1, "Starting and Stopping Components." For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, start Node Manager as soon as possible so that the entries get encrypted.

14.5.3.2.6 Configuring Managed WebLogic Servers to Use the Custom Keystores Follow these steps to configure the identity and trust keystores for *WLS_SERVER*:

1. Log in to Oracle WebLogic Server Administration Console for the for the domain which is being extended at: the address specified in Section 15.2, "About Identity and Access Management Console URLs."
2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Click the name of the server for which you want to configure the identity and trust keystores (*WLS_SERVER*). The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. In the Keystores field, select the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates.
8. In the Identity section, define attributes for the identity keystore:
   - **Custom Identity Keystore:** The fully qualified path to the identity keystore:

     SHARED_CONFIG`/keystores/appIdentityKeyStore.jks`

   - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
   - **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in Section 14.5.3.2.4, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.
9. In the Trust section, define properties for the trust keystore:

- **Custom Trust Keystore:** The fully qualified path to the trust keystore:

  SHARED_CONFIG/keystores/appTrustKeyStoreNEWHOST.jks

- **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
- **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in Section 14.5.3.2.4, "Creating a Trust Keystore Using the Keytool Utility" This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.

10. Click **Save**.
11. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
12. Select **Configuration**, then **SSL**.
13. Click **Lock and Edit**.
14. In the **Private Key Alias** field, enter the alias you used for the host name the Managed Server listens on, for example: `appIdentityNEWHOST`

    In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 14.5.3.2.3, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."
15. Click **Save**.
16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
17. Restart the server for which the changes have been applied, as described in Section 15.1, "Starting and Stopping Components."

14.5.3.2.7 Changing the Host Name Verification Setting for the Managed Servers

Once the previous steps have been performed, set host name verification for the affected Managed Servers to `Bea Hostname Verifier`. To do this, perform the following steps in both the IAMAccessDomain and IAMGovernanceDomain:

1. Log in to Oracle WebLogic Server Administration Console. (Console URLs are provided in Section 15.2, "About Identity and Access Management Console URLs.")
2. Select **Lock and Edit** from the change center.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select the Managed Server in the Names column of the table. The settings page for the server is displayed.
6. Open the SSL tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `Bea Hostname Verifier`.
9. Click **Save**.
10. Click **Activate Changes**.

14.5.3.2.8 Starting Node Manager Run the following commands to start Node Manager.

```
cd SHARED_CONFIG/nodemanager/hostname
./startNodeManagerWrapper.sh
```

Note: Verify that Node Manager is using the appropriate stores and alias from the Node Manager output. You should see the following when Node Manager starts.:

```
<Loading identity key store:
  FileName=ASERVER_HOME/keystores/appIdentityKeyStore.jks,
Type=jks, PassPhraseUsed=true>
```

Host name verification works if you apply a test configuration change to the servers and it succeeds without Node Manager reporting any SSL errors.

15

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the Identity and Access Management topology. These operations include monitoring, scaling, backing up your topology, and troubleshooting.

This chapter includes the following topics:

15.1 Starting and Stopping Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment.

This section contains the following topics:

15.1.1 Startup Order

When starting up your entire infrastructure, start the components in the following order, (ignoring those not in your topology):

1. Database(s)
2. Database Listener(s)
3. LDAP hosts

4. OAM hosts
5. OIM hosts
6. Web hosts
7. Oracle Identity Manager Managed servers
8. Identity Access Domain WebLogic Administration Server
9. Oracle Access Management Access Manager Server(s)
10. OAAM Administration Server
11. OAAM Managed Server (if OAAM is part of the topology)
12. Oracle HTTP Server(s)

15.1.2 Starting and Stopping All Servers by Using a Script

During Deployment, scripts were created in the *SHARED_CONFIG_DIR*/config/scripts directory to start and stop all the servers in the environment. Two of the scripts are available for you to use from the command line to start and stop all Identity and Access Management servers. The remaining scripts are used internally and must not be invoked from the command line.

Note: These scripts do NOT stop or start the database.

15.1.2.1 Starting All Servers

Deployment created a file called `startall.sh`, which is used to start all of the components on a particular server. To start everything in the correct order run the command on hosts in the following order:

Consolidated Topology

- LDAPHOST1
- LDAPHOST2
- IAMHOST1
- IAMHOST2
- WEBHOST1
- WEBHOST2

Distributed Topology

- LDAPHOST1
- LDAPHOST2
- OAMHOST1
- OIMHOST1
- OAMHOST2
- OIMHOST2
- WEBHOST1
- WEBHOST2

If you want to start the services on a single host, execute the command on that host.

During exectution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

The script starts the components which are installed on a given host in the following order. What is started depends on what is installed on the host on which the script is running:

1. Oracle Unified Directory
2. Node Manager
3. Administration Server(s)
4. SOA Managed Server
5. OIM Managed Server
6. OAM Managed Server
7. Oracle HTTP Server
8. OAAM Managed Server

15.1.2.2 Stopping All Servers:

The script to stop all servers is `stopall.sh`.

Run the command on hosts in the reverse of the order used to start all servers.

During exectution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

15.1.3 Manually Starting and Stopping Identity and Access Management Components

Start and Stop individual Identity and Access Management components as described in the following subsections:

15.1.3.1 Starting and Stopping Oracle Unified Directory

Start and stop Oracle Unified Directory as follows:

15.1.3.1.1 Starting Oracle Unified Directory To start Oracle Unified Directory issue the following command:

```
OUD_ORACLE_INSTANCE/OUD/bin/start-ds
```

15.1.3.1.2 Stopping Oracle Unified Directory To stop Oracle Unified Directory issue the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/stop-ds
```

15.1.3.2 Starting an Oracle Access Manager Managed Servers When None is Running

Normally, you start Access Manager managed servers by using the WebLogic console. After you have enabled Single Sign-On for the administration consoles, however, you must have at least one Access Manager Server running in order to access a console. If no Access Manager server is running, you can start one by using WLST.

To invoke WLST on Linux or UNIX, type:

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./wlst.sh
```

Once you are in the WLST shell, execute the following commands:

```
nmConnect('Admin_User','Admin_Password', 'OAMHOST','Port', 'domain_name','IAD_
MSERVER_HOME')
nmStart('wls_oam1')
```

where *Port* is *NMGR_PORT*, *domain_name* is the name of the domain and *Admin_User* and *Admin_Password* are the Node Manager username and password. For example:

```
nmConnect('weblogic','password', 'OAMHOST1','5556', 'IAMAccessDomain','IAD_
MSERVER_HOME')
```

If an Access Manager Managed server is already running then you can start the Access Manager Managed server as you would any other web logic managed server via the WebLogic Administration console.

15.1.3.3 Starting and Stopping a WebLogic Administration Server

Start and stop a WebLogic Administration Server as described in the following sections.

Notes:

- *Admin_User* and *Admin_Password* are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the file: *IAD_ASERVER_HOME*/config/nodemanager/nm_password.properties
- If you are starting the IAMAccessDomain Administration server, *ASERVER_HOME* is *IAD_ASERVER_HOME*. If you are starting the IAMGovernanceDomain Administration server, *ASERVER_HOME* is *IGD_ASERVER_HOME*

15.1.3.3.1 Starting a WebLogic Administration Server The recommended way to start the Administration server is to use WLST and connect to Node Manager:

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Where *ORACLE_COMMON_HOME* is from the *MW_HOME* associated with the domain you are starting or stopping.

To start the Administration Server in the Access Domain, use the following command:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','IAD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain')
nmStart('AdminServer')
```

Execute the following command to start the Administration Server in the Governance Domain:

```
nmConnect('Admin_User','Admin_Password','IGDADMINVHN','5556',
```

```
'IAMGovernanceDomain','IGD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('weblogic','password', 'IADADMINVHN','5556', 'IAMAccessDomain','IAD_
MSERVER_HOME')
```

Alternatively, you can start the Administration server by using the command:

```
ASERVER_HOME/bin/startWebLogic.sh
```

15.1.3.3.2 Stopping a WebLogic Administration Server To stop the Administration Server, log in to the WebLogic console using the URL listed in Chapter 15.2, "About Identity and Access Management Console URLs."

Then proceed as follows:

1. Click the **Control** tab.
2. Select **AdminServer(admin)**.
3. Click **Shutdown** and select **Force Shutdown now**.
4. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

15.1.3.4 Starting and Stopping WebLogic Managed Servers

Start and stop managed servers as follows.

15.1.3.4.1 Starting WebLogic Managed Servers To start a managed server, log in to the WebLogic console using the URL listed in Chapter 15.2, "About Identity and Access Management Console URLs."

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select managed server for example **wls_oim1**
4. Click the **Start** button.
5. Click **Yes** when asked to confirm that you want to start the server(s).

15.1.3.4.2 Stopping WebLogic Managed Servers To stop a Managed Server(s), log in to the WebLogic console using the URL listed in Chapter 15.2, "About Identity and Access Management Console URLs." Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select Managed Server for example **wls_oim1**
4. Click the **Shutdown** button and select **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

15.1.3.5 Starting and Stopping Node Manager

Start and stop Node Manager as follows.

15.1.3.5.1 Starting Node Manager If the Node Manager being started is the one that controls the Administration Server, then prior to starting the Node Manager issue the command:

```
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
```

To start Node Manager, issue the commands:

```
cd SHARED_CONFIG_DIR/nodemanager/hostname
./startNodeManagerWrapper.sh
```

15.1.3.5.2 Stopping Node Manager To stop Node Manager, kill the process started in the previous section.

15.2 About Identity and Access Management Console URLs

Table 15–1 lists the administration consoles used in this guide and their URLs.

Table 15–1 Console URLs

Domain	Console	URL	User Name
IAMAccessDomain	WebLogic Administration Console	http://IADADMIN.mycompany.com/console	weblogic_idm
	Enterprise Manager FMW Control	http://IADADMIN.mycompany.com/em	weblogic_idm
	Access Management console	http://IADADMIN.mycompany.com/oamconsole	oamadmin
	OAAM Server	https://SSO.mycompany.com/oaam_server	n/a
	OAAM Administration Console	http://IADADMIN.mycompany.com/oaam_admin	oaamadmin
IAMGovernanceDomain	WebLogic Administration Console	http://IGDADMIN.mycompany.com/console	weblogic_idm
	Enterprise Manager FMW Control	http://IGDADMIN.mycompany.com/em	weblogic_idm
	Identity Manager System Administration Console	http://IGDADMIN.mycompany.com/sysadmin	xelsysadm
	Identity Manager Self Service Console	https://SSO.mycompany.com/identity	xelsysadm
	Authorization Policy Manager	http://IGDADMIN.mycompany.com/apm	oamadmin

15.3 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 15.3.1, "Monitoring Oracle Unified Directory"
- Section 15.3.2, "Monitoring WebLogic Managed Servers"

15.3.1 Monitoring Oracle Unified Directory

You can check the status of Oracle Unified Directory by issuing the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/status
```

This command accesses the locally running Oracle Unified Directory instance and reports the status of the directory, including whether or not replication and LDAP or LDAPS is enabled.

15.3.2 Monitoring WebLogic Managed Servers

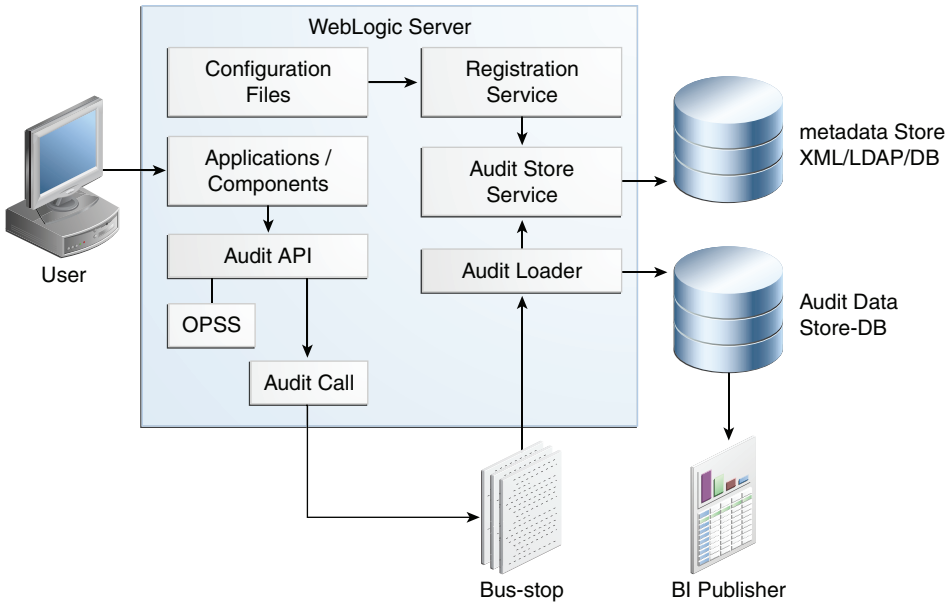
You can use Oracle Enterprise Manager Fusion Middleware Control to monitor Managed Servers and other Fusion Middleware components, such as Access Manager, Oracle Identity Manager, Oracle Identity Federation, and SOA. For more information, see the administrator guides listed in the Preface under "Related Documents".

15.4 Auditing Identity and Access Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications are able to create application-specific audit events. For non-JavaEE Oracle components in the middleware such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

Figure 15–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework. For more information, see *Oracle Fusion Middleware Application Security Guide*.

Figure 15–1 Audit Event Flow



The Oracle Fusion Middleware Audit Framework consists of the following key components:

- Audit APIs

  These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run-time, applications may call these APIs where appropriate to audit the necessary information about a particular event happening in the application code. The interface enables applications to specify event details such as username and other attributes needed to provide the context of the event being audited.

- Audit Events and Configuration

  The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also enables applications to define application-specific events.

  These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WLST (command-line tool).

- The Audit Bus-stop

  Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are periodically uploaded to the audit repository based on a configurable time interval.

- Audit Loader

  As the name implies, audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit

loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.

- Audit Repository

  Audit Repository contains a pre-defined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and grow over time. Ideally, this should not be an operational database used by any other applications - rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (Oracle RAC) database as the audit data store.

- Oracle Business Intelligence Publisher

  The data in the audit repository is exposed through pre-defined reports in Oracle Business Intelligence Publisher. The reports enable users to drill down the audit data based on various criteria. For example:

  - Username
  - Time Range
  - Application Type
  - Execution Context Identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware Application Security Guide*.

For information on how to configure the repository for Oracle Fusion Middleware Audit Framework, see the "Configuring and Managing Auditing" chapter in the *Oracle Fusion Middleware Application Security Guide*.

The EDG topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader are available once the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

15.5 Performing Backups and Recoveries

You can use the UNIX `tar` command for most backups. Typical usage is:

```
tar -czvpsPf BACKUP_LOCATION/backup_file.tar directories
```

You can use the UNIX `tar` command for recovery. Typical usage is:

```
tar -xzvpsPf BACKUP_LOCATION/backup_file.tar
```

For database backup and recovery, you can use the database utility RMAN. See the *Oracle Database Backup and Recovery Reference* for more information on using this command.

This section contains the following topics:

- Section 15.5.1, "Peforming Baseline Backups"

- Section 15.5.2, "Performing Runtime Backups"
- Section 15.5.3, "Performing Backups During Installation and Configuration"

15.5.1 Peforming Baseline Backups

Perform baseline backups when building a system and when applying patches that update static artifacts, such as the Oracle binaries.

After performing a baseline backup, also perform a runtime backup.

Table 15–2 Static Artifacts to Back Up in the Identity and Access Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	Oracle RAC database hosts: IAMDBHOST1 IAMDBHOST2	User Defined	Database
Oracle Unified Directory Binaries	LDAPHOST1 LDAPHOST2	Middleware Home: `DIR_MW_HOME`	Directory Tier
Oracle Access Management Binaries	OAMHOST1 OAMHOST2	Middleware Home: *`IAD_MW_HOME`*	Application Tier
Oracle Identity Governance Binaries	OIMHOST1 OIMHOST2	Middleware Home: *`IGD_MW_HOME`*	Application Tier
Web Tier Binaries	WEBHOST1 WEBHOST2	Middleware Oracle home, *`WEB_ORACLE_HOME`*:	Web Tier
Install-Related Files	Each host	OraInventory: *`ORACLE_BASE`*`/oraInventory` `/etc/oratab`, `/etc/oraInst.loc` `~/bea/beahomelist` (on hosts where WebLogic Server is installed)	Not applicable.

Note: It is also recommended that you back up your load balancer configuration. Refer to your vendor documentation on how to do this.

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

15.5.2 Performing Runtime Backups

Perform runtime backups on an ongoing basis. These backups contain information on items that can change frequently, such as data in the database, domain configuration information, and identity information in LDAP directories.

Table 15–3 Run-Time Artifacts to Back Up in the Identity and Access Management Enterprise Deployments

Type	Host	Location	Tier
IAMAccessDomain Home	OAMHOST1 OAMHOST2	Administration Server and Shared Files: *IAD_ASERVER_HOME* Managed Servers: *IAD_MSERVER_HOME*	Application Tier
IAMGovernanceDomain Home	OIMHOST1 OIMHOST2	Administration Server and Shared Files: *IGD_ASERVER_HOME* Managed Servers: *IGD_MSERVER_HOME*	Application Tier
Oracle HTTP Server	WEBHOST1 WEBHOST2	*WEB_ORACLE_INSTANCE*	Web Tier
Oracle RAC Databases	IAMDBHOST1 IAMDBHOST2	User defined	Directory Tier
Oracle Unified Directory	LDAPHOST1 LDAPHOST2	*OUD_ORACLE_INSTANCE*	Application Tier

15.5.3 Performing Backups During Installation and Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process.

For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

This section contains the following topics:

- Section 15.5.3.1, "Backing Up Middleware Home"
- Section 15.5.3.2, "Backing Up LDAP Directories"
- Section 15.5.3.3, "Backing Up the Database"
- Section 15.5.3.4, "Backing Up the WebLogic Domain IAMGovernanceDomain"
- Section 15.5.3.5, "Backing Up the WebLogic Domain IAMAccessDomain"
- Section 15.5.3.6, "Backing Up the Web Tier"

15.5.3.1 Backing Up Middleware Home

Back up the Middleware homes whenever you create a new one or add components to it. The Middleware homes used in this guide are Oracle Identity Management and Oracle Identity and Access Management, as listed in Table 15–2.

15.5.3.2 Backing Up LDAP Directories

Whenever you perform an action which updates the data in LDAP, back up the directory contents.

This section contains the following topics:

- Section 15.5.3.2.1, "Backing Up Oracle Unified Directory"
- Section 15.5.3.2.2, "Backing Up Third-Party Directories"

15.5.3.2.1 Backing Up Oracle Unified Directory To backup Oracle Unified Directory, perform the following steps:

1. Shut down the Oracle Unified Directory Instances as described in Section 15.1, "Starting and Stopping Components."
2. Back up *OUD_ORACLE_INSTANCE* directories on each host.
3. Restart the Oracle Unified Directory instances as described in Section 15.1, "Starting and Stopping Components."

15.5.3.2.2 Backing Up Third-Party Directories Refer to your operating system vendor's documentation for information about backing up directories.

15.5.3.3 Backing Up the Database

Whenever you create add a component to the configuration, back up the IAMDB database. Perform this backup after creating domains or adding components such as Oracle Access Management Access Manager or Oracle Identity Manager.

15.5.3.4 Backing Up the WebLogic Domain IAMGovernanceDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 15.1, "Starting and Stopping Components."
2. Back up the *IGD_ASERVER_HOME* directory from shared storage.
3. Back up the *IGD_MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

15.5.3.5 Backing Up the WebLogic Domain IAMAccessDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 15.1, "Starting and Stopping Components."
2. Back up the *IAD_ASERVER_HOME* directory from shared storage.
3. Back up the *IAD_MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

15.5.3.6 Backing Up the Web Tier

To back up the Web Tier, perform these steps:

15.5.3.6.1 Backing Up Oracle HTTP Server Back up Oracle HTTP Server as follows:

1. Shut down the Oracle HTTP Server as described in Section 15.1, "Starting and Stopping Components."
2. Back up the *WEB_ORACLE_INSTANCE* directory on local storage.
3. Start the Oracle HTTP Server as described in Section 15.1, "Starting and Stopping Components."

15.6 Patching Enterprise Deployments

It is recommended that you patch enterprise deployments by using the automated patching solution included with the Identity and Access Management Lifecycle Tools.

The process of applying patches can be summarized as follows:

1. Create a patch top. A patch top directory contains patches, classified by each product to which patches apply.
2. Run Patch Manager to generate a patch plan. Based on the deployment topology and patches provided, the Manager creates an optimal plan to apply those patches.
3. Run the Patcher against all hosts which are affected by the plan. You might need to execute the Patcher on a given host multiple times if required by a given plan. As each Patcher invocation completes, it directs you where to run the Patcher next.

When the Patcher runs, it stops and starts server instances as necessary, and ensures that patches are applied in the correct order to satisfy dependencies.

Full details on how to use the IDM Patching Framework can be found in *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*. The Guide also contains instructions for patching the deployment manually if required, using the OPatch tool.

15.7 Preventing Timeouts for SQL

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall so it does not time out these connections. If such a configuration is not possible, set the SQLNET.EXPIRE_TIME=n parameter in the *ORACLE_HOME*`/network/admin/sqlnet.ora` file on the database server, where `n` is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

15.8 Manually Failing Over the WebLogic Administration Server

This section discusses how to fail over the Administration Server to a new host after the primary host fails. The example in this section shows how to fail the Access Management Administration Server from OAMHOST1 to OAMHOST2. If you are failing over the Oracle Identity Manager Administration server, substitute the appropriate values for that domain.

This section contains the following topics:

15.8.1 Failing Over the Administration Server to OAMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from OAMHOST1 to OAMHOST2.

Assumptions:

- The Administration Server is configured to listen on `IADADMINVHN.mycompany.com`, and not on `ANY` address.
- The Administration Server is failed over from OAMHOST1 to OAMHOST2, and the two nodes have these IP addresses:
  - OAMHOST1: `100.200.140.165`
  - OAMHOST2: `100.200.140.205`
  - IADADMINVHN: `100.200.140.206`

    This is the Virtual IP address where the Administration Server is running, assigned to *interface*:*index* (for example, eth1:2), available in OAMHOST1 and OAMHOST2.
- The domain directory where the Administration Server is running in OAMHOST1 is on a shared storage and is mounted also from OAMHOST2.

  Note: NM in OAMHOST2 does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on OAMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, Node Manager is fully functional
- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed in OAMHOST2 as described in previous chapters. That is, the same path for *`IAD_ORACLE_HOME`* and *`IAD_MW_HOME`* that exists in OAMHOST1 is available in OAMHOST2.

The following procedure shows how to fail over the Administration Server to a different node, OAMHOST2.

1. Stop the Administration Server on OAMHOST1 as described in Section 15.1, "Starting and Stopping Components."
2. Migrate the IP address to the second node.
   a. Run the following command as root on OAMHOST1 (where *x*:*y* is the current interface used by `IADADMINVHN.mycompany.com`):

      `/sbin/ifconfig x:y down`

      For example:

      `/sbin/ifconfig eth0:1 down`

   b. Run the following command on OAMHOST2:

      `/sbin/ifconfig interface:index IP_Address netmask netmask`

      For example:

      `/sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0`

> **Note:** Ensure that the netmask and interface to be used match the available network configuration in OAMHOST2.

3. Update routing tables by using `arping` on OAMHOST2, for example:

```
/sbin/arping -q -U -c 3 -I eth0 100.200.140.206
```

15.8.2 Starting the Administration Server on OAMHOST2

Perform the following steps to start Node Manager on OAMHOST2.

1. On OAMHOST2, mount the Administration Server domain directory if it is not already mounted. For example:

```
mount /u01/oracle
```

2. Start Node Manager by using the following commands:

```
cd WL_HOME/server/bin
./startNodeManager.sh
```

3. Stop the Node Manager by killing the Node Manager process.

> **Note:** Starting and stopping Node Manager at this point is only necessary the first time you run Node Manager. Starting and stopping it creates a property file from a predefined template. The next step adds properties to that property file.

4. Run the setNMProps.sh script to set the `StartScriptEnabled` property to `true` before starting Node Manager:

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

> **Note:** You must use the `StartScriptEnabled` property to avoid class loading failures and other problems.

5. Start the Node Manager as described in Section 15.1, "Starting and Stopping Components."

6. Start the Administration Server on OAMHOST2.

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in the WLST shell, execute the following commands:

```
nmConnect('admin','Admin_Password', 'OAMHOST2','5556',
'IAMAccessDomain','/u1/oracle/config/domains/IAMAccessDomain')
nmStart('AdminServer')
```

7. Test that you can access the Administration Server on OAMHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console at:

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

b. Check that you can access and verify the status of components in the Oracle Enterprise Manager at: `http://IADADMINVHN.mycompany.com/em`.

15.8.3 Validating Access to OAMHOST2 Through Oracle HTTP Server

Perform the same steps as in Section 11.1.1, "Verify Connectivity" This is to check that you can access the Administration Server when it is running on OAMHOST2.

15.8.4 Failing the Administration Server Back to OAMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on OAMHOST2 and run it on OAMHOST1. To do this, migrate IADADMINVHN back to OAMHOST1 node as described in the following steps.

1. Ensure that the Administration Server is not running on OAMHOST2. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from *IAD_ASERVER_HOME*`/bin`.
2. On OAMHOST2, unmount the Administration server domain directory. For example:

   ```
   umount /u01/oracle
   ```

3. On OAMHOST1, mount the Administration server domain directory. For example:

   ```
   mount /u01/oracle
   ```

4. Disable the `IADADMINVHN.mycompany.com` virtual IP address on OAMHOST2 and run the following command as `root` on OAMHOST2:

   ```
   /sbin/ifconfig x:y down
   ```

   where *x*:*y* is the current interface used by `IADADMINVHN.mycompany.com`.

5. Run the following command on OAMHOST1:

   ```
   /sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
   ```

   Note: Ensure that the netmask and interface to be used match the available network configuration in OAMHOST1

6. Update routing tables by using arping. Run the following command from OAMHOST1.

   ```
   /sbin/arping -q -U -c 3 -I interface 100.200.140.206
   ```

7. If Node Manager is not already started on OAMHOST1, start it, as described in Section 15.1, "Starting and Stopping Components."
8. Start the Administration Server again on OAMHOST1.

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./wlst.sh
   ```

   Once in the WLST shell, execute

   ```
   nmConnect(admin,'Admin_Pasword, OAMHOST1,'5556',
        'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain'
   nmStart('AdminServer')
   ```

9. Test that you can access the Oracle WebLogic Server Administration Console at:

   `http://IADADMINVHN.mycompany.com:7001/console`

   where `7001` is *`WLS_ADMIN_PORT`* in Section 7.1, "Assembling Information for Identity and Access Management Deployment."

10. Check that you can access and verify the status of components in the Oracle Enterprise Manager at:

    `http://IADADMIN.mycompany.com/em`

15.9 Changing Startup Location

When the environment was deployed, start and stop scripts were generated to start and stop components in the topology. At the time of Deployment, the Access Domain Administration server was configured to start on OAMHOST1. If you want to permanently change this to start on OAMHOST2, perform the following steps.

Use the same steps, changing the name of the server and host, to change the Governance Domain Administration server to start on OIMHOST2 instead of OIMHOST1.

Edit the file `serverInstancesInfo.txt`, which is located in the directory: *`SHARED_CONFIG_DIR`*`/scripts`

Locate the line which looks like this:

```
OAMHOST1.mycompany.com AS AdminServer
```

Change `OAMHOST1` to `OAMHOST2` and save the file.

15.10 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 15.10.1, "Troubleshooting Identity and Access Management Deployment"
- Section 15.10.2, "Troubleshooting Start/Stop Scripts"
- Section 15.10.3, "Troubleshooting Oracle Oracle Access Management Access Manager 11g"
- Section 15.10.4, "Troubleshooting Oracle Identity Manager"
- Section 15.10.5, "Troubleshooting Oracle SOA Suite"

15.10.1 Troubleshooting Identity and Access Management Deployment

This section describes some common problems related to Deployment. It contains the following topics:

- Section 15.10.1.1, "Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute"
- Section 15.10.1.2, "Deployment Fails"

15.10.1.1 Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute

Problem

Deployment fails with an error similar to this:

```
Incorrect host format for attibute : PRIMARY_OAM_SERVERS :
server-123.mycompany.com
```

Due to a bug, one of the tools invoked during the deployment process cannot handle host names or domain names containing the hyphen (-) character.

Solution

Use host names and domain names that do NOT contain the hyphen (-) character.

15.10.1.2 Deployment Fails

Problem

Deployment fails.

Solution

Check the Deployment logs located in the directory:

LCM_HOME/provisioning/logs/*hostname*

where *hostname* is the host where the Deployment step failed.

15.10.2 Troubleshooting Start/Stop Scripts

This section describes some common problems related to Start/Stop scripts. It contains the following topics:

- Section 15.10.2.1, "Preverify Inappropriately Fails with Insufficient Space"
- Section 15.10.2.2, "Start/Stop Scripts Fail to Start or Stop a Managed Server"

15.10.2.1 Preverify Inappropriately Fails with Insufficient Space

Problem

When preverify runs, it checks that sufficient space is available in the directory *IDM_TOP*. If you have created separate mount points for *IDM_TOP*/products and *IDM_TOP*/config, preverify does not add together the space allocated to the two mount points and fails the check inappropriately.

Solution

Disable the free space check by editing the file:

LCM_HOME/provisioning/idm-provisioning-build/idm-common-preverify-build.xml

Locate the entry:

```
<target name="common-preverify-tasks">
```

Comment out the following entry so that after editing it looks like this:

```
<!--antcall target="private-preverify-free-space"/-->
```

Save the file.

15.10.2.2 Start/Stop Scripts Fail to Start or Stop a Managed Server

Problem

Problem: Start/Stop scripts fail to start or stop a managed server.

The start/stop logs in the directory *SHARED_CONFIG_DIR*/scripts/logs contain an error similar to this:

```
weblogic.utils.AssertionError: ***** ASSERTION FAILED *****
        at
weblogic.server.ServerLifeCycleRuntime.getStateRemote(ServerLifeCycleRuntime.java:
734)
        at
weblogic.server.ServerLifeCycleRuntime.getState(ServerLifeCycleRuntime.java:581)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

Solution

1. Shut down the failing managed server. You might have to kill the process.
2. Back up the managed server's LDAP data, then remove it. For example:

   ```
   rm -rf LOCAL_CONFIG_DIR/domains/IAMAccessDomain/servers/server_name/data/ldap
   ```

   where *server_name* is the name of the failing managed server.
3. Restart the managed server.

15.10.3 Troubleshooting Oracle Oracle Access Management Access Manager 11g

This section describes some common problems that can arise with Access Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 15.10.3.1, "Access Manager Runs out of Memory"
- Section 15.10.3.2, "User Reaches the Maximum Allowed Number of Sessions"
- Section 15.10.3.3, "Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed"
- Section 15.10.3.4, "You Are Not Prompted for Credentials After Accessing a Protected Resource"
- Section 15.10.3.5, "Cannot Log In to Access Management Console"

15.10.3.1 Access Manager Runs out of Memory

Problem

After Access Manager has been running for a while, you see the following error message in the output:

```
Attempting to allocate 1G bytes
There is insufficient native memory for the Java Runtime Environment to continue.
```

Possible reasons:

- The system is out of physical RAM or swap space.

- In 32 bit mode, the process size limit was reached.

Solutions

- Reduce memory load on the system.
- Increase physical memory or swap space.
- Check if swap backing store is full.
- Use 64 bit Java on a 64 bit OS.
- Decrease Java heap size (-Xmx/-Xms).
- Decrease number of Java threads.
- Decrease Java thread stack sizes (-Xss).
- Disable compressed references (-XXcompressedRefs=false).
- Ensure that command line tool `adrci` can be executed from the command line.
  - at oracle.dfw.impl.incident.ADRHelper.invoke(ADRHelper.java:1309)
  - at oracle.dfw.impl.incident.ADRHelper.createIncident(ADRHelper.java:929
  - at oracle.dfw.impl.incident.DiagnosticsDataExtractorImpl.createADRIncident(DiagnosticsDataExtractorImpl.java:1116)
- On both OAMHOST1 and OAMHOST2, edit the file `setSOADomainEnv.sh`, which is located in *`IAD_MSERVER_HOME`*`/bin` and locate the line which begins:

  ```
  PORT_MEM_ARGS=
  ```

  Change this line so that it reads:

  ```
  PORT_MEM_ARGS="-Xms768m -Xmx2560m"
  ```

15.10.3.2 User Reaches the Maximum Allowed Number of Sessions

Problem

The Access Manager server displays an error message similar to this:

```
The user has already reached the maximum allowed number of sessions. Please close
one of the existing sessions before trying to login again.
```

Solution

If users log in multiple times without logging out, they might overshoot the maximum number of configured sessions. You can modify the maximum number of configured sessions by using the Access Management Administration Console.

To modify the configuration by using the Access Management Administration Console, proceed as follows:

1. Go to **System Configuration** -> **Common Settings** -> **Session**
2. Increase the value in the **Maximum Number of Sessions per User** field to cover all concurrent login sessions expected for any user. The range of values for this field is from 1 to any number.

15.10.3.3 Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed

Problem

The Administration Server takes a long time to start after configuring Access Manager.

Solution

Tune the Access Manager database. When the Administration server first starts after configuring Access Manager, it creates a number of default policies in the database. If the database is distant or in need of tuning, this can take a significant amount of time.

```
Resources
Authentication Policies
   Protected Higher Level Policy
   Protected Lower Level Policy
   Publicl Policy
Authorization Policies
   Authorization Policies
```

If you do not see these items, the initial population has failed. Check the Administration Server log file for details.

15.10.3.4 You Are Not Prompted for Credentials After Accessing a Protected Resource

Problem

When you access a protected resource, Access Manager should prompt you for your user name and password. For example, after creating a simple HTML page and adding it as a resource, you should see credential entry screen.

Solution

If you do not see the credential entry screen, perform the following steps:

1. Verify that Host Aliases for IAMAccessDomain have been set. You should have aliases for `IAMAccessDomain`:80, `IAMAccessDomain`:Null, `IADADMIN.mycompany.com:80`, and `SSO.mycompany.com:443`, where Port `80` is *`HTTP_PORT`* and Port `443` is *`HTTP_SSL_PORT`*.
2. Verify that WebGate is installed.
3. Verify that `ObAccessClient.xml` was copied from *`IAD_ASERVER_HOME`*`/output` to the WebGate Lib directory and that OHS was restarted.
4. When `ObAccessClient.xml` was first created, the file was not formatted. When the OHS is restarted, reexamine the file to ensure that it is now formatted. OHS gets a new version of the file from Access Manager when it first starts.
5. Shut down the Access Manager servers and try to access the protected resource. You should see an error saying Access Manager servers are not available. If you do not see this error, re-install WebGate.

15.10.3.5 Cannot Log In to Access Management Console

Problem

You cannot log in to the Access Management Console. The Administration Server diagnostic log might contain an error message similar to this:

```
Caused by: oracle.security.idm.OperationFailureException:
oracle.security.am.common.jndi.ldap.PoolingException [Root exception is
oracle.ucp.UniversalConnectionPoolException:
Invalid life cycle state.
 Check the status of the Universal Connection Pool]
        at
oracle.security.idm.providers.stdldap.UCPool.acquireConnection(UCPool.java:112)
```

Solution

Remove the /tmp/UCP* files and restart the Administration Server.

15.10.4 Troubleshooting Oracle Identity Manager

This section describes some common problems that can arise with Oracle Identity Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 15.10.4.1, "java.io.FileNotFoundException When Running Oracle Identity Manager Configuration"
- Section 15.10.4.2, "ResourceConnectionValidationxception When Creating User in Oracle Identity Manager"
- Section 15.10.4.3, "Oracle Identity Manager Reconciliation Jobs Fail"

15.10.4.1 java.io.FileNotFoundException When Running Oracle Identity Manager Configuration

Problem

When you run Oracle Identity Manager configuration, the error `java.io.FileNotFoundException: soaconfigplan.xml (Permission denied)` may appear and Oracle Identity Manager configuration might fail.

Solution

To workaround this issue:

1. Delete the file `/tmp/soaconfigplan.xml`.
2. Start the configuration again (`OH/bin/config.sh`).

15.10.4.2 ResourceConnectionValidationxception When Creating User in Oracle Identity Manager

Problem

If you are creating a user in Oracle Identity Manager (by logging into Oracle Identity Manager System Administration Console, clicking the Administration tab, clicking the **Create User** link, entering the required information in the fields, and clicking **Save**) in an active-active Oracle Identity Manager configuration, and the Oracle Identity Manager server that is handling the request fails, you may see a "ResourceConnectionValidationxception" in the Oracle Identity Manager log file, similar to:

```
[2010-06-14T15:14:48.738-07:00] [oim_server2] [ERROR] [] [XELLERATE.SERVER]
[tid: [ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: xelsysadm] [ecid:
004YGJGmYrtEkJV6u3M6UH00073A0005EI,0:1] [APP: oim#11.1.1.3.0] [dcid:
12eb0f9c6e8796f4:-785b18b3:12938857792:-7ffd-0000000000000037] [URI:
```

```
/admin/faces/pages/Admin.jspx] Class/Method:
PooledResourceConnection/heartbeat encounter some problems: Operation timed
out[[
com.oracle.oim.gcp.exceptions.ResourceConnectionValidationxception: Operation
timed out
        at
oracle.iam.ldapsync.impl.repository.LDAPConnection.heartbeat(LDAPConnection.ja
va:162)
        at
com.oracle.oim.gcp.ucp.PooledResourceConnection.heartbeat(PooledResourceConnec
tion.java:52)
         .
         .
         .
```

Solution

Despite this exception, the user is created correctly.

15.10.4.3 Oracle Identity Manager Reconciliation Jobs Fail

Problem

Oracle Identity Manager reconciliation jobs fail, or the following message is seen in the log files:

```
LDAP Error 53 : [LDAP: error code 53 - Full resync required. Reason: The provided
cookie is older than the start of historical in the server for the replicated
domain : dc=mycompany,dc=com]
```

This error is caused by the data in the Oracle Unified Directory change log cookie expiring because Oracle Unified Directory has not been written to for a certain amount of time.

Solution:

1. Open a browser and go to the following location:

   ```
   http://igdadmin.mycompany.com/sysasdmin
   ```

2. Log in a as `xelsysadm` using the *`COMMON_IDM_PASSWORD`*.
3. Under **System Management**, click **Scheduler**.
4. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
5. For each job in the search results, click on the job name on the left, then click **Disable** on the right.

   Do this for all jobs. If the job is already disabled do nothing.

6. Run the following commands on LDAPHOST1:

   ```
   cd OUD_ORACLE_INSTANCE/OUD/bin
   ./ldapsearch -h ldaphost1 -p 1389 -D "cn=oudadmin" -b "" -s base
   "objectclass=*" lastExternalChangelogCookie

   Password for user 'cn=oudadmin': <OudAdminPwd>
   dn: lastExternalChangelogCookie:
   dc=mycompany,dc=com:00000140c682473c263600000862;
   ```

Copy the output string that follows `lastExternalChangelogCookie:`. This value is required in the next step. For example,

```
dc=mycompany,dc=com:00000140c682473c263600000862;
```

The Hex portion must be 28 characters long. If this value has more than one Hex portion then separate the 28char portions with spaces. For example:

```
dc=mycompany,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
```

7. Run each of the following LDAP reconciliation jobs once to reset the last change number.:
   - LDAP Role Delete Reconciliation
   - LDAP User Delete Reconciliation
   - LDAP Role Create and Update Reconciliation
   - LDAP User Create and Update Reconciliation
   - LDAP Role Hierarchy Reconciliation
   - LDAP Role Membership Reconciliation

   To run the jobs:

   a. Login to the OIM System Administration Console as the user `xelsysadm`.
   b. Under **System Management**, click **Scheduler**.
   c. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
   d. Click on the job to be run.
   e. Set the parameter **Last Change Number** to the value obtained in step 6.

      For example:

      ```
      dc=mycompany,dc=com:00000140c4ceb0c07a8d00000043
      00000140c52bd0b9104200000042 00000140c52bd0ba17b9000002ac
      00000140c3b290b076040000012c;
      ```

   f. Click **Run Now**.
   g. Repeat for each of the jobs in the list at the beginning of this step.
8. For each incremental recon job whose last changelog number has been reset, execute the job and check that the job now completes successfully.
9. After the job runs successfully, re-enable periodic running of the jobs according to your requirements.

If the issue continues to occur, increase the cookie retention time to two months by running the following command on each OUD instance.

If, the error appears again after the incremental jobs have been re-enabled and run successfully ("Full resync required. Reason: The provided cookie is older..."), then increase the OUD cookie retention time. Although there is no hard and fast rule as to what this value should be, it should be long enough to avoid the issue, but small enough to avoid unnecessary resource consumption on OUD. One or two weeks should suffice; two week is given in the following example:

```
./dsconfig set-replication-server-prop --provider-name "Multimaster
Synchronization" --set replication-purge-delay:8w -D cn=oudadmin --trustAll -p
```

```
4444 -h LDAPHOST1

Password for user 'cn=oudadmin':  <OudAdminPswd>
Enter choice [f]: f
```

15.10.5 Troubleshooting Oracle SOA Suite

This section describes some common problems that can arise with Oracle SOA Suite and the actions you can take to resolve the problem. It contains the following topics:

15.10.5.1 Transaction Timeout Error

Problem: The following transaction timeout error appears in the log:

```
Internal Exception: java.sql.SQLException: Unexpected exception while enlisting
 XAConnection java.sql.SQLException: XA error: XAResource.XAER_NOTA start()
failed on resource 'SOADataSource_soaedg_domain': XAER_NOTA : The XID
is not valid
```

Solution: Check your transaction timeout settings, and be sure that the JTA transaction time out is less than the DataSource XA Transaction Timeout, which is less than the `distributed_lock_timeout` (at the database).

With the out of the box configuration, the SOA data sources do not set XA timeout to any value. The `Set XA Transaction Timeout` configuration parameter is unchecked in the WebLogic Server Administration Console. In this case, the data sources use the domain level JTA timeout which is set to `30`. Also, the default `distributed_lock_timeout` value for the database is `60`. As a result, the SOA configuration works correctly for any system where transactions are expected to have lower life expectancy than such values. Adjust these values according to the transaction times your specific operations are expected to take.

A

Automation of the Process

This appendix describes how to write a scripts to invoke all of the scripts from a single host.

It is possible to write a script to invoke all of the scripts from a single host, in effect creating a one command deployment.

Below are sample scripts which can be modified to achieve this.

> **Disclaimer:** These scripts are example implementations and are provided as is as a proof of concept to demonstrate a method to automate the deployment process. The scripts must be customized and tested for the specific need of your environment.

This appendix includes the following topics:

A.1 setenv.sh

This script sets the environment.

```
#!/bin/sh
#
# setenv.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#     setenv.sh - captures details of environment to be deployed
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
#
#    NOTES
#      <other useful comments, qualifications, etc.>
#
#    MODIFIED   (MM/DD/YY)
#
CURRENT_HOST=`hostname`
```

```
export USERNAME=<unix user eg oracle>

export IDMTOP=SW_ROOT
export SHARED_CONFIG_DIR=$IDMTOP/config
export LOCAL_CONFIG_DIR=<LOCAL_ROOT>
export REPOSITORY=<REPOS_HOME>
export INSTALLERS=$REPOSITORY/installers
export RESPONSE_FILE=<FULLY QUALIFIED PATH TO DEPLOYMENT RESPONSE FILE>
export PROVISIONING=<IDMLCM_HOME>/provisioning
export SCRIPTS_DIR=<DIRECTORY CONTAINING THESE SCRIPTS>
export JAVA_HOME=$REPOSITORY/jdk6
export ANT_HOME=$REPOSITORY/provisioning/ant
export PRIMORDIAL_TO_DMZ_SHARE=$PROVISIONING/dmzShare

export RCU_HOME=$INSTALLERS/rcu
export RCU_LOG_LOCATION=$SCRIPTS_DIR/rcu/logs-$$
export RCU_LOG_NAME=rcu.log
export RCU_TIMESTAMP_LOG_DIR=false
export DB_SCHEMA_PREFIX=DEV

PHASES_TO_RUN='preverify install preconfigure configure configure-secondary
postconfigure startup validate'

export ALL_HOSTS='<LDAPHOST1> <LDAPHOST2> <OAMHOST1> <OAMHOST2> <OIMHOST1>
<OIMHOST2> <WEBHOST1> <WEBHOST2>'

export DB_CONNECT_STRING=<DB-SCAN>:<DB_LSNR_PORT>:<IDSTORE_SERVICE_NAME>
export DB_PASSWORD_SYS=<DB SYS PWD>
export DB_PASSWORD_SCHEMA=<RCU_SCHEMA_PASSWORD>

mkdir -p $PRIMORDIAL_TO_DMZ_SHARE

function timer()
{
    if [[ $# -eq 0 ]]; then
        echo $(date '+%s')
    else
        local  stime=$1
        etime=$(date '+%s')

        if [[ -z "$stime" ]]; then stime=$etime; fi
        dt=$((etime - stime))
        ds=$((dt % 60))
        dm=$(((dt / 60) % 60))
        dh=$((dt / 3600))
        printf '%d:%02d:%02d' $dh $dm $ds
    fi
}

 execCmd()
 {
   HOST=$1
   shift
   CMD_LINE=$*
   CMD="ssh $USERNAME@$HOST $CMD_LINE"

  echo "[idmprov] " `date` $CMD
  tmr=$(timer)
  $CMD
```

```
  printf '[idmprov] Elapsed time: %s\n' $(timer $tmr)
}
```

A.2 setlocalenv.sh

```
#!/bin/sh
#
# setlocalenv.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#     setenv.sh - captures details of environment to be deployed
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
#
#    NOTES
#      <other useful comments, qualifications, etc.>
#
#    MODIFIED   (MM/DD/YY)

#
CURRENT_HOST=`hostname`

export USERNAME=<software owner>

export IDMTOP=<SW_ROOT>
export SHARED_CONFIG_DIR=$IDMTOP/config
export LOCAL_CONFIG_DIR=<LOCAL_ROOT>
export REPOSITORY=<REPOS_HOME>
export INSTALLERS=$REPOSITORY/installers
export RESPONSE_FILE=<FULLY QUALIFIED PATH TO DEPLOYMENT RESPONSE FILE>
export PROVISIONING=<IDMLCM_HOME>/provisioning
export SCRIPTS_DIR=<DIRECTORY CONTAINING THESE SCRIPTS>
export JAVA_HOME=$REPOSITORY/jdk6
export ANT_HOME=$REPOSITORY/provisioning/ant
export PRIMORDIAL_TO_DMZ_SHARE=$PROVISIONING/dmzShare
```

A.3 deploy.sh

This is the Deployment script.

```
#!/bin/sh
#
# deploy.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#      provision.sh - this script starts executing Deployment phases in all hosts
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
#
#    NOTES
```

```
#      - copy all scripts named prov_*.sh to a directory in primordial host
#      - make sure this directory is accessible using the same path from all hosts
being provisioned
#      - update prov_env.sh with environment specific details (directories,
hostnames, db, etc)
#      - run this script from the primordial host
#      - script will create one log file for each phase in each host - named prov_
run-<phase>-<host>.log
#      - script will stop when Deployment completes or on detecting 1st failure
(absence of "BUILD SUCCESSFUL" in the log file)
#
#    MODIFIED   (MM/DD/YY)
#

. <DIRECTORY CONTAINING THESE SCRIPTS>/setenv.sh

if [ ! -e $SCRIPTS_DIR/logs ]
then
     mkdir -p $SCRIPTS_DIR/logs
fi

rm -r $SCRIPTS_DIR/logs/* LCM_ROOT/provisioning* <LCM_ROOT>/internal LCM_
ROOT/lcmconfig LCM_ROOT/keystores 2> /dev/null

starttmr=$(timer)

for PHASE in $PHASES_TO_RUN
do
  phasetmr=$(timer)
  for HOST in $ALL_HOSTS
  do
    echo "[idmprov] Running $PHASE on  $HOST"
    logFile=$SCRIPTS_DIR/logs/$PHASE-$HOST.log

    execCmd $HOST ". $SCRIPTS_DIR/setlocalenv.sh; cd $PROVISIONING/bin;
./runIAMDeployment.sh -responseFile $RESPONSE_FILE -target $PHASE" > $logFile

    fgrep -s "BUILD SUCCESSFUL" $logFile
    if [ "$?" = "1" ]
    then
        echo "ERROR: $PHASE failed in $HOST"
        exit 1
    fi

  done

  echo -e "[idmprov] Total $PHASE\c"
  printf ' time: %s\n' $(timer $phasetmr)
done

printf '[idmprov] Total Elapsed time: %s\n' $(timer $starttmr)
```

A.4 Using the Scripts

Use the scripts as follows:

1. Copy the scripts to a location that is available on each host in the topology.

2. Edit the scripts and replace entries like `<SW_ROOT>` with entries applicable to your environment. Use Section 7.1, "Assembling Information for Identity and Access Management Deployment," to assist with this.
3. Set up `ssh` equivalence from the primordial host to each of the other hosts in the topology. See your operating system documentation for details.
4. Validate that `ssh` equivalence is working by issuing the following command from the primordial host to each host in the topology. This command should show the date on each remote machine without any prompts:

   ```
   ssh hostname date
   ```

5. Copy the deployment response file generated in Chapter 8, "Creating a Deployment Profile," to the same directory where these scripts are located.
6. Run the `deploy.sh` script.
7. After deployment is complete, remove the `ssh` equivalence.

B

Cleaning Up an Environment Before Rerunning IAM Deployment

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

When you provision Oracle Identity and Access Management using the `runIAMDeployment.sh` command, you must complete each stage in the topology before beginning the next stage, in a specified order. 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. To do this, you should restart the host.
2. On each host, remove the contents of the directory *`LOCAL_ROOT`*.
3. Remove the contents of the directory IDM_TOP on shared storage.

> **Note:** In this example, *SHARED_CONFIG_DIR* is nested under *IDM_TOP*. As a result, it is also deleted. However, if you have *SHARED_CONFIG_DIR* in a different location, delete it explicitly as well.

4. If you are using Oracle Internet Directory instead of Oracle Unified Directory as the directory host, drop the database schema using RCU.

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

C

Topology Tool Commands for Scaling

This appendix describes useful `topotool.sh` commands for scaling an Identity and Access Management enterprise deployment.

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Lifecycle Tools read the store in order to build and execute the patch plan.

Chapter 14, "Scaling Enterprise Deployments" describes how to scale the deployment up or out using a variety of tools. As part of a scaling procedure, you must add new entries to the store covering the new additions to the deployment. This is done using the IAM Topology Tool.

The tool is located at: *IDMLCM_HOME*`/topotool/bin`

Before running the Topology Tool, back up your entire *LCM_ROOT*`/lcmconfig/topology` directory.

> **Note:** Many of the command-line options use instance or component names that include numbers, for example `OUD3`. You should already have determined these names when you assembled information for scaling. See the Assembling Information sections in Chapter 14, "Scaling Enterprise Deployments."

This chapter contains the following sections:

- Section C.1, "Syntax of the Topology Tool"
- Section C.2, "Commonly-Used Command Line Operations"
- Section C.3, "Steps and Command-Line Examples"

C.1 Syntax of the Topology Tool

The general syntax is:

```
topotool.sh command [-option]
```

For help, use:

```
topotool.sh [-help]

topotool.sh command [-help]
```

Note: This section is not a complete description of the syntax of the Topology Tool. The commands and options listed in this section include only those that are used in this guide.

C.1.1 Commands

Add

Adds information to the topology store.

```
topotool.sh add [options]
```

Modify

Modifies information in the topology store.

```
topotool.sh modify [options]
```

C.1.2 Command-Line Options Used with Add

-component

Specifies adding of a component.

-confighomename oud*n* | oim*n* | oam*n* | soa*n* | NodeManager:Access | NodeManager:Identity | ohs*n*

Specifies a local or shared configuration home to add. Used with `-instance`.

-dbname *DBNAME*

Specifies the Oracle Database to use. Used with `-instance`. In this guide, *`DBNAME`* is always `OIM:DB`.

-description *STRING*

Used with `-machine` and `-confighome`. *`STRING`* is a quoted string, such as `"oim3 machine"`.

-fqdn *HOSTNAME*

Specifies a host. The *`HOSTNAME`* format is a fully qualified domain name, such as `ldaphost3.mycompany.com`, `oimhost4.mycompany.com`. Used with `-host`.

-hometype OUD | IAM | SOA | WEBTIER

Specifies the home type to be added. Used with `-instance`.

-host

Specifies adding a host.

-instance

Specifies adding an instance.

-instancegroup *STRING*

Specifies an instance group. In this guide, *STRING* is always `1` when used with `-instancegroup`. Used with `-instance`.

-machine

Specifies adding a machine

-machinename *MACHINE*

Specifies the machine to be added. Used with `-instance` and `-machine`. The format of *MACHINE* is a fully qualified machine name such as `ldaphost3.mycompany.com`, `oimhost4.mycompany.com`.

-mwhomename Directorytier:MW_HOME | Access:MW_HOME | Identity:MW_HOME | Webtier:MW_HOME | Webtier:MW_HOME_2 | Webtier:MW_HOME_*n*

Specifies the Middleware home to add. Used with `-instance`

-name *NAME*

Specifies the name of a machine or an instance. When used with `-machine`, the *NAME* format is a fully-qualified hostname, such as `ldaphost3.mycompany.com`.

When used with `-instance` or `-confighome`, the *NAME* format is *`productn`*, for example `oid3`.

When used with `-instance`, the *NAME* format is a hostname and port pair, in the format *`productn`*`:`*`host`*`:plain` for a non-SSL port and *`productn`*`:`*`host`*`:ssl` for an SSL port, where *`product`* is a component, such as `OUD` or `OIM`, and *`n`* is the instance number.

When used to add an OPMN instance the hostname part of the *NAME* format is `OPMN`, for example: `OPMN:webhost3:ssl`.

-path *PATH*

Specifies a quoted directory path, such as `"/u01/oracle/config/nodemanager/oimhost3.mycompany.com"`. Used with `-confighome`

-port *PORT*

Specifies a port number, such as 5556. Used with `-host`.

-secure true | false

Set to `true` for an SSL port and `false` for a non-SSL port. Used with `-host`.

-shared true | false

used with `-confighome` to indicate whether this is a shared or local configuration home.

-sharedlcmconfigaccessible true | false

Specifies whether the shared LCM configuration is accessible. Used with `-machine`. In this guide, it is set to `true` when adding application tier machines and to `false` for web tier machines.

-tier DIRECTORY | IDM | WEB |

Specifies the tier, as listed in Chapter 14, "Scaling Enterprise Deployments."

-type TYPE

Specifies the type of an instance or a component. In both cases, **TYPE** stands for the specific type definition to be used, matching the instance or component being added.

When used with `-instance`, the value can be one of: OUD | OHS_HTTPD | OPMN WLS_ADMIN | WLS_MANAGED | WLS_NODE_MANAGER

When used with `-component`, the value can be one of: OHS_WEBGATE | WLS_ADMIN_OAM_CONSOLE | WLS_ADMIN_WLS_CONSOLE | WLS_MANAGED_OAM | WLS_MANAGED_OIM | WLS_MANAGED_SOA

-virtual true | false

Specifies whether the host being added is a virtual host. Used with `-host`. It is always `false` in this guide.

C.1.3 Command-Line Options Used with Modify for Updating Load Balancer Mappings

-lbrmapping

Specifies modification of the load balancer mapping by the addition of a new host

-lbrname *LBRNAME*

Used with `-lbrmapping`. Specifies the name of the load balancer. *`LBRNAME`* is always `LBR1` or `LBR2` in this guide.

-name idstore | idstore_ssl

Used with `-lbrmapping`. Specifies the load balancer mapping name.

-physicalhosts *HOSTS*

Used with `-lbrmapping`. Specifies a host or a comma-separated list of hosts. For a non-SSL host, the format is *`productn`*`:`*`host`*, for example: `OUD:LDAP:oud1:ldaphost1,oud2:ldaphost2,oud3:ldaphost3`. For an SSL host, the format is *`productn`*`:`*`host`*`:ssl`, for example: oud3:ldaphost3:ssl

C.2 Commonly-Used Command Line Operations

Adding a Machine:

```
topotool.sh add -machine -name MACHINE -sharedlcmconfigaccessible true_false
```

Adding a Non-SSL Host:

```
topotool.sh add -host -name HOST -fqdn FQDN -port PORT -secure false -virtual
false
```

Adding an SSL Host:

```
topotool.sh add -host -name HOST_SSL -fqdn FQDN -port SSL_PORT -secure false
-virtual false
```

Adding a Local Configuration Home:

```
topotool.sh add -confighome -name LOCAL_CONFIG -path PATH -shared false
```

Adding a Shared Configuration Home:

```
topotool.sh add -confighome -name SHARED_CONFIG -path
"/u01/oracle/config/instances/oud3" -shared true
```

Adding an Instance:

```
topotool.sh add -instance -machinename MACHINE -name INSTANCE -type TYPE -tier
TIER -mwhomename MWHOME-hometype  -confighomename  LOCAL_OR_SHARED_CONFIG
-instancegroup 1
```

Adding a Component:

```
topotool.sh add -component -instancename INSTANCE -type TYPE -hosts HOST
```

Updating LBR Mappings:

```
topotool.sh modify -lbrmapping -lbrname LBR -name LBR_MAPPING -physicalhosts HOST
topotool.sh modify -lbrmapping -lbrname LBR_SSL -name LBR_MAPPING -physicalhosts
HOST_SSL
```

C.3 Steps and Command-Line Examples

This section contains notes about each tier, general steps for scaling out the components in that tier, and example command lines. It contains the following topics:

- Section C.3.1, "Scaling Out / Scaling Up of Directory Tier"
- Section C.3.2, "Scaling Out / Scaling Up of Application Tier"
- Section C.3.3, "Scaling Out / Scaling Up of Web Tier"

Note: Do not use the examples directly. You must substitute the values with your own data.

C.3.1 Scaling Out / Scaling Up of Directory Tier

The following sections provide information about scaling the directory tier.

- Section C.3.1.1, "Directory Tier Notes"
- Section C.3.1.2, "Topology Tool Steps for Scaling Oracle Unified Directory"
- Section C.3.1.3, "Scale Out Commands for Oracle Unified Directory"
- Section C.3.1.4, "Scale Up Commands for Oracle Unified Directory"

C.3.1.1 Directory Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the LDAP hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.
- Reconfigure load balancer mappings.

C.3.1.2 Topology Tool Steps for Scaling Oracle Unified Directory

1. Add a machine with `sharedlcmconfigaccessible` set to true. (Only for scale out).
2. Add a non-SSL host if Oracle Unified Directory is listening on non-SSL port.
3. Add a SSL host if Oracle Unified Directory is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type OUD, tier DIRECTORY, hometype OUD using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Update the load balancer mappings with the newly created non-SSL or SSL hosts.

C.3.1.3 Scale Out Commands for Oracle Unified Directory

- Adding new machine

```
topotool.sh add -machine -name ldaphost3.mycompany.com -description "oud3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.mycompany.com
-port 1389 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn
ldaphost3.mycompany.com -port 1390 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oud3 -description "oud3 local
configuration home" -path "/u02/private/oracle/config/instances/oud3"
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oud3 -description "oud3 configuration
home" -path "/u01/oracle/config/instances/oud3" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename ldaphost3.mycompany.com -name oud3
-description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
HOME -hometype OUD -confighomename oud3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
oud3:ldaphost3,oud3:ldaphost3:ssl
```

- Adding the new host to the load balancer mappings
  - Non-SSL:

```
topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
```

```
oud3:ldaphost3
```

- SSL:

```
topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
-physicalhosts oud3:ldaphost3:ssl
```

C.3.1.4 Scale Up Commands for Oracle Unified Directory

- Adding new machine

```
topotool.sh add -machine -name ldaphost3.mycompany.com -description "oud3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.mycompany.com
-port 1389 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn
ldaphost3.mycompany.com -port 1390 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oud3 -description "oud3 local
configuration home" -path "/u02/private/oracle/config/instances/oud3"
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oud3 -description "oud3 configuration
home" -path "/u01/oracle/config/instances/oud3" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename ldaphost3.mycompany.com -name oud3
-description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
HOME -hometype OUD -confighomename oud3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
oud3:ldaphost3,oud3:ldaphost3:ssl
```

- Adding the new host to the load balancer mappings
  - Non-SSL:

```
topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
oud3:ldaphost3
```

  - SSL:

```
topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
-physicalhosts oud3:ldaphost3:ssl
```

C.3.2 Scaling Out / Scaling Up of Application Tier

The following sections provide information about scaling the application tier.

C.3.2.1 Application Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.
- Node manager added in case of Scale Out.

C.3.2.2 Topology Tool Steps for OAM

1. Add a machine with `sharedlcmconfigaccessible` set to `true`. (Only for scale out).
2. Add a non-SSL host if OAM is listening on non-SSL port.
3. Add a SSL host if OAM is listening on SSL port.
4. Add a host for OAP.
5. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
6. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
7. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
8. Add a component for the newly created instance of type WLS_MANAGED_OAM using the newly created non-SSL or SSL hosts.

C.3.2.3 Scale Out Commands for OAM

- Adding new machine

```
topotool.sh add -machine -name oamhost3.mycompany.com -description "oam3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

```
topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.mycompany.com
-port 14100 -secure false -virtual false
```

- SSL:

```
topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.mycompany.com
-port 14101 -secure true -virtual false
```

- Adding the new host for OAP (hostname + port combination)

```
topotool.sh add -host -name oam3:slc03oap3 -fqdn oamhost3.mycompany.com -port
5575 -secure false -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oam3 -description "oam3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oam3 -description "oam3 shared
configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.mycompany.com -name oam3
-description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
-hometype IAM -confighomename oam3 -dbname OIM:DB -domainname  IAMAccessDomain
-instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
oam3:oamhost3,oam3:oamhost3:ssl
```

C.3.2.4 Scale Up Commands for OAM

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

```
topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.mycompany.com
-port 14100 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.mycompany.com
-port 14101 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oam3 -description "oam3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oam3 -description "oam3 shared
configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.mycompany.com -name oam3
-description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
-hometype IAM -confighomename oam3 -dbname OIM:DB -domainname  IAMAccessDomain
-instancegroup 1
```

- Adding component

```
topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
oam3:oamhost3,oam3:oamhost3:ssl
```

C.3.2.5 Topology Tool Steps for OIM

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if OIM is listening on non-SSL port.
3. Add a SSL host if OIM is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_OIM using the newly created non-SSL or SSL hosts.

C.3.2.6 Scale Out commands for OIM

- Adding new machine

```
topotool.sh add -machine -name oimhost3.mycompany.com -description "oim3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

```
topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.mycompany.com
-port 14000 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.mycompany.com
-port 14001 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oim3 -description "oim3 local
configuration home" -path
```

```
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

- Shared config:

```
topotool.sh add -confighome -name oim3 -description "oim3 shared
configuration home" -path "
/u01/oracle/config/domains/IAMGovernanceDomain"-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.mycompany.com -name oim3
-description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
IAMGovernanceDomain -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
oim3:oimhost3,oim3:oimhost3:ssl

topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
oim3:oimhost3,oim3:oimhost3:ssl
```

C.3.2.7 Scale Up commands for OIM

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

```
topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.mycompany.com
-port 14000 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.mycompany.com
-port 14001 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oim3 -description "oim3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oim3 -description "oim3 shared
configuration home" -path "
/u01/oracle/config/domains/IAMGovernanceDomain"-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.mycompany.com -name oim3
-description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
IAMGovernanceDomain -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
oim3:oimhost3,oim3:oimhost3:ssl
```

```
topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
oim3:oimhost3,oim3:oimhost3:ssl
```

C.3.2.8 Topology Tool Steps for SOA

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if SOA is listening on non-SSL port.
3. Add a SSL host if SOA is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype SOA using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_SOA using the newly created non-SSL or SSL hosts.

C.3.2.9 Scale Out commands for SOA

- Adding new machine

```
topotool.sh add -machine -name oimhost3.mycompany.com -description "soa3
instance machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

```
topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.mycompany.com
-port 8001 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.mycompany.com
-port 8002 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name soa3 -description "soa3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name soa3 -description "soa3 shared
configuration home" -path "
/u01/oracle/config/domains/IAMGovernanceDomain"-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.mycompany.com -name soa3
-description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
IAMGovernanceDomain -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
soa3:oimhost3,soa3:oimhost3:ssl

topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
soa3:oimhost3,soa3:oimhost3:ssl
```

C.3.2.10 Scale Up Commands for SOA

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.mycompany.com
    -port 8001 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.mycompany.com
    -port 8002 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name soa3
  -description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
  soa3:oimhost3,soa3:oimhost3:ssl

  topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
  soa3:oimhost3,soa3:oimhost3:ssl
  ```

C.3.2.11 Steps for Adding Node Manager Steps for OAM/OIM/SOA Scale Out Only

1. Add a non-SSL host if Node Manager is listening on non-SSL port.
2. Add a SSL host if Node Manager is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
4. Add an instance of type WLS_NODE_MANAGER, tier IDM, hometype IAM using an existing middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.

6. Add a component for the newly created instance of type WLS_NODE_MANAGER using the newly created non-SSL or SSL hosts.

C.3.2.12 Commands for Adding NodeManager for Scale Out of OAM

- Adding new host (hostname + port combination) for Node Manager OAM
  - Non-SSL:

```
topotool.sh add -host -name NodeManager:oamhost3 -fqdn
oamhost3.mycompany.com -port 5556 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name NodeManager:oamhost3:ssl -fqdn
oamhost3.mycompany.com -port 5556 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name NodeManager:Access -description "node
manager local configuration home" -path
"/u01/oracle/config/nodemanager/oamhost3.mycompany.com" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name NodeManager:Access -description " node
manager shared configuration home " -path
"/u01/oracle/config/nodemanager/oamhost3.mycompany.com" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.mycompany.com -name
NodeManager:Access -description "node manager  instance" -type WLS_NODE_MANAGER
-tier IDM -mwhomename Access:IAD_MW_HOME -hometype IAM -confighomename
NodeManager:Access  -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename NodeManager:Access -type DEFAULT
-hosts NodeManager:oamhost3, NodeManager:oamhost3:ssl
```

C.3.2.13 Commands for Adding NodeManager for Scale Out of OIM

- Adding new host (hostname + port combination) for Node Manager OIM
  - Non-SSL:

```
topotool.sh add -host -name NodeManager:oimhost3 -fqdn
oimhost3.mycompany.com -port 5556-secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
oimhost3.mycompany.com -port 5556 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name NodeManager:Identity -description "node
manager local configuration home" -path
"/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared false
```

- Shared config:

```
topotool.sh add -confighome -name NodeManager:Identity -description " node
manager shared configuration home " -path
"/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.mycompany.com -name
NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
-confighomename NodeManager:Identity  -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
-hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
```

C.3.2.14 Commands for Adding NodeManager for Scale Out of SOA

- Adding new host (hostname + port combination) for Node Manager SOA
  - Non-SSL:

```
topotool.sh add -host -name NodeManager:oimhost3 -fqdn
oimhost3.mycompany.com -port 5556-secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
oimhost3.mycompany.com -port 5556 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name NodeManager:Identity -description "node
manager local configuration home" -path
"/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name NodeManager:Identity -description " node
manager shared configuration home " -path
"/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.mycompany.com -name
NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
-confighomename NodeManager:Identity  -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
-hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
```

C.3.3 Scaling Out / Scaling Up of Web Tier

The following sections provide information about scaling the web tier.

C.3.3.1 Web Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries not shared. They are local.
- The config directory is not mounted.
- Reconfigure Load Balancer.

C.3.3.2 Topology Tool Steps for Scaling OHS

1. Add a machine with sharedlcmconfigaccessible set to false. (Only for scale out).
2. Add a non-SSL host if OHS is listening on non-SSL port.
3. Add a SSL host if OHS is listening on SSL port.
4. Add a new Middleware Home with shared set as false. (Only for scale out)
5. Add a new Oracle Home. (Only for scale out)
6. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
7. Add an instance of type OHS_HTTPD, tier WEB, hometype WEBTIER using the newly created middleware home or existing middleware home in case of scale up.
8. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
9. Add a component for the newly created instance of type OHS_WEBGATE using the newly created non-SSL or SSL hosts.
10. Update the SSO, IDMINTERNAL, OIMADMIN, OAMADMIN load balancer mappings with the newly created non-SSL or SSL hosts.

C.3.3.3 Scale Out Commands for Web

- Adding new machine

```
topotool.sh add -machine -name webhost3.mycompany.com -description "ohs3
machine" -sharedlcmconfigaccessible false
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.mycompany.com
-port 7777 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.mycompany.com
-port 7778 -secure true -virtual false
```

- Adding new MW Home(s)

  ```
  topotool.sh add -mwhome -name Webtier:WEB_MW_HOME -path
  /u01/oracle/idmtop/products/ohs/ -shared false
  ```

- Adding new Oracle Home(s)

  ```
  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type ORACLE_COMMON -path
  /u01/oracle/idmtop/products/ohs/oracle_common

  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type WEBTIER -path
  /u01/oracle/idmtop/products/ohs/ohs

  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type OAM_WG -path
  /u01/oracle/idmtop/products/ohs/webgate
  ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 local
    configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
    -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 shared
    configuration home" -path " /u02/private/oracle/config/instances/ohs3"
    -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name ohs3
  -description "ohs3 instance" -type OHS_HTTPD -tier WEB -mwhomename Webtier:WEB_
  MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
  ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

  topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
  ohs3:webhost3,ohs3:webhost3:ssl
  ```

- Adding the new host to the load balancer mappings
  - Adding to sso LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to idminternal LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name idminternal
    -physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oimadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oamadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

C.3.3.4 Scale Up Commands for OHS

- Adding new host (hostname + port combination)
  - Non-SSL:

    ```
    topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.mycompany.com
    -port 7777 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.mycompany.com
    -port 7778 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 local
    configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
    -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 shared
    configuration home" -path " /u02/private/oracle/config/instances/ohs3"
    -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name ohs3
  -description "ohs3" -type OHS_HTTPD -tier WEB -mwhomename Webtier:MW_HOME
  -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
  ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

  topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
  ohs3:webhost3,ohs3:webhost3:ssl
  ```

- Adding the new host to the load balancer mappings
  - Adding to sso LBR Mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name sso  -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to idminternal LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name idminternal
    -physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oimadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oamadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

C.3.3.5 Steps for Adding OPMN for Webtier Scale Up and Scale Out

1. Add a non-SSL host if OPMN is listening on non-SSL port.
2. Add a SSL host if OPMN is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
4. Add an instance of type OPMN, tier WEB, hometype WEBTIER using an existing web tier middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.

C.3.3.6 Commands for Adding OPMN Instance for WEB Tier for Scale Out and Scale Up

- Adding new host (hostname + port combination)
  - Non-SSL:

    ```
    topotool.sh add -host -name OPMN:ohs3 -fqdn webhost3.mycompany.com -port
    6700 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name OPMN:webhost3:ssl -fqdn webhost3.mycompany.com
    -port 6701 -secure true -virtual false
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name OPMN:ohs3
  -description "opmn for ohs third instance" -type OPMN -tier WEB -mwhomename
  Webtier:MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename OPMN:ohs3 -type DEFAULT -hosts
  OPMN:webhost3, OPMN:webhost3:ssl
  ```