Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity Management
(Oracle Fusion Applications Edition)

11*g* Release 1 (11.1.1.5.0)

E21032-01

August 2011

ORACLE®

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition), 11*g* Release 1 (11.1.1.5.0)

E21032-01

Contents

3   Configuring the Database Repositories

4   Installing the Software

8   Extending the Domain with Oracle Directory Integration Platform and ODSM

9   Extending the Domain with Oracle Virtual Directory

10   Preparing Directories Other than Oracle Internet Directory

11   Preparing Identity and Policy Stores

12   Extending the Domain with Oracle Access Manager 11g

13 Extending the Domain with Oracle Identity Manager

14   Extending the Domain with Oracle Identity Federation

15   Setting Up Node Manager

16   Configuring Server Migration for Oracle Identity Manager

17 Integrating Components

18 Configuring Single Sign-on for Administration Consoles

19   Managing Enterprise Deployments

Index

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 Management* (*Fusion Applications Edition*).

Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Fusion Middleware 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 Administrator's Guide*

- *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*

- *Oracle Fusion Middleware Application Security Guide*

- *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*

- *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*

- *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*

- *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 Fusion Middleware Administrator's Guide for Oracle Identity Federation*

- *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*

For additional information about Oracle Fusion Applications, consult the following documents in the Oracle Fusion Applications library:

- *Oracle Fusion Applications Administrator and Implementor Roadmap*

- *Oracle Fusion Applications Administrator's Guide*

- *Oracle Fusion Applications Enterprise Deployment 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.

1

Enterprise Deployment Overview

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

Deploying Oracle Identity Management as described in this guide is a prerequisite for deploying Oracle Fusion Applications as described in *Oracle Fusion Applications Enterprise Deployment Guide*.

This chapter includes the following topics:

- Section 1.1, "What is an Enterprise Deployment?"
- Section 1.2, "Terminology"
- Section 1.3, "Benefits of Oracle Recommendations"
- Section 1.4, "The Enterprise Deployment Reference Topologies"
- Section 1.5, "Understanding the Topology Tiers"
- Section 1.6, "Using This Guide"

1.1 What is an Enterprise Deployment?

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, Oracle Collaboration Suite, and Oracle Grid 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, visit:

http://www.oracle.com/technetwork/database/features/availability/maa-090890.html

1.2 Terminology

Table 1–1 provides definitions for some terms that define the architecture of an Oracle Fusion Middleware environment:

Table 1–1   Oracle Fusion Middleware Architecture Terminology

Term	Definition
Oracle Fusion Middleware home	A **Middleware home** consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes.
	A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
WebLogic Server home	A **WebLogic Server home** contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of other Oracle home directories underneath the Middleware home directory.
Oracle home	An **Oracle home** contains installed files necessary to host a specific product. For example, the Oracle Identity Management Oracle home contains a directory that contains binary and library files for Oracle Identity Management.
	An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.
Oracle instance	An **Oracle instance** contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. The system components in an Oracle instance must reside on the same machine. An Oracle instance directory contains updatable files, such as configuration files, log files, and temporary files.
	An Oracle instance is a peer of an Oracle WebLogic Server domain. Both contain specific configurations outside of their Oracle homes.
	The directory structure of an Oracle instance is separate from the directory structure of the Oracle home. It can reside anywhere; it need not be within the Middleware home directory.

Table 1–1   (Cont.) Oracle Fusion Middleware Architecture Terminology

Term	Definition
Oracle WebLogic Server domain	A **WebLogic Server domain** is a logically related group of Java components. A WebLogic Server domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional WebLogic Server instances called Managed Servers. You deploy Java components, such as Web applications, EJBs, and Web services, and other resources to the Managed Servers and use the Administration Server for configuration and management purposes only.
	Managed Servers in a WebLogic Server domain can be grouped together into a cluster.
	An Oracle WebLogic Server domain is a peer of an Oracle instance. Both contain specific configurations outside of their Oracle homes.
	The directory structure of an WebLogic Server domain is separate from the directory structure of the WebLogic Server home. It can reside anywhere; it need not be within the Middleware home directory.
system component	A **system component** is a manageable process that is not WebLogic Server. For example: Oracle HTTP Server, WebCache, and Oracle Internet Directory. Includes the JSE component.
Java component	A **Java component** is a peer of a system component, but is managed by the application server container. Generally refers to a collection of applications and resources, with generally a 1:1 relationship with a domain extension template. For example: SOA and WebCenter Spaces.
Oracle Fusion Middleware farm	Oracle Enterprise Manager Fusion Middleware Control is a Web browser-based, graphical user interface that you can use to monitor and administer an Oracle Fusion Middleware farm.
	An **Oracle Fusion Middleware farm** is a collection of components managed by Fusion Middleware Control. It can contain WebLogic Server domains, one or more Managed Servers and the Oracle Fusion Middleware system components that are installed, configured, and running in the domain.

1.3 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:

- Section 1.3.1, "Built-in Security"
- Section 1.3.2, "High Availability"

1.3.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own DMZ, 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 is redirected to port 443.
- 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 DMZ is allowed.
- Components are separated between DMZs on the web tier, application tier, and the directory 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.
- Oracle Internet Directory is isolated in the directory tier DMZ.
- Identity Management components are in the application tier DMZ.
- All communication between components across DMZs is restricted by port and protocol, according to firewall rules.

1.3.2 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.

1.4 The Enterprise Deployment Reference Topologies

Oracle Identity Management consists of a number of products, which can be used either individually or collectively. The Enterprise Deployment Guide for Identity Management (Fusion Applications Edition) enables you to build two different enterprise topologies for Fusion Applications. This section provides diagrams of the topologies.

- Section 1.4.1, "Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications"
- Section 1.4.2, "Oracle Identity Federation 11g for Fusion Applications"

> **Note:** Customers who use machines with large memory and CPU foot prints can collapse multiple machines in the topology into single machines.

1.4.1 Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications

Figure 1–1 is a diagram of the Oracle Access Manager 11*g* and Oracle Identity Manager 11*g* topology.

Figure 1–1   Oracle Access Manager 11g and Oracle Identity Manager 11g *for Fusion Applications*
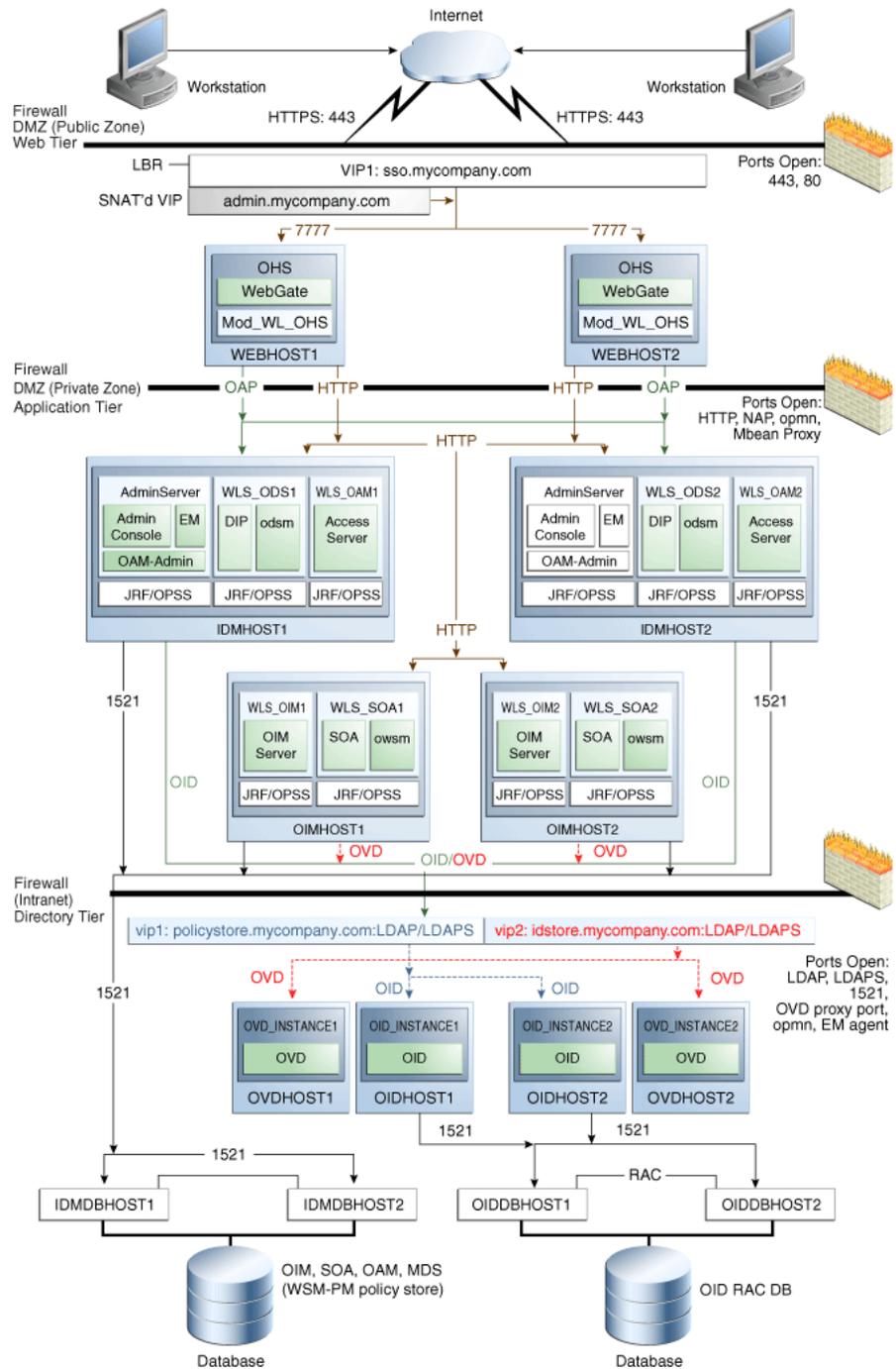
1.4.2 Oracle Identity Federation 11g for Fusion Applications

Figure 1–2 is a diagram of the Oracle Identity Federation 11 *g* topology for Fusion Applications.

Figure 1–2   Oracle Identity Federation 11g Topology
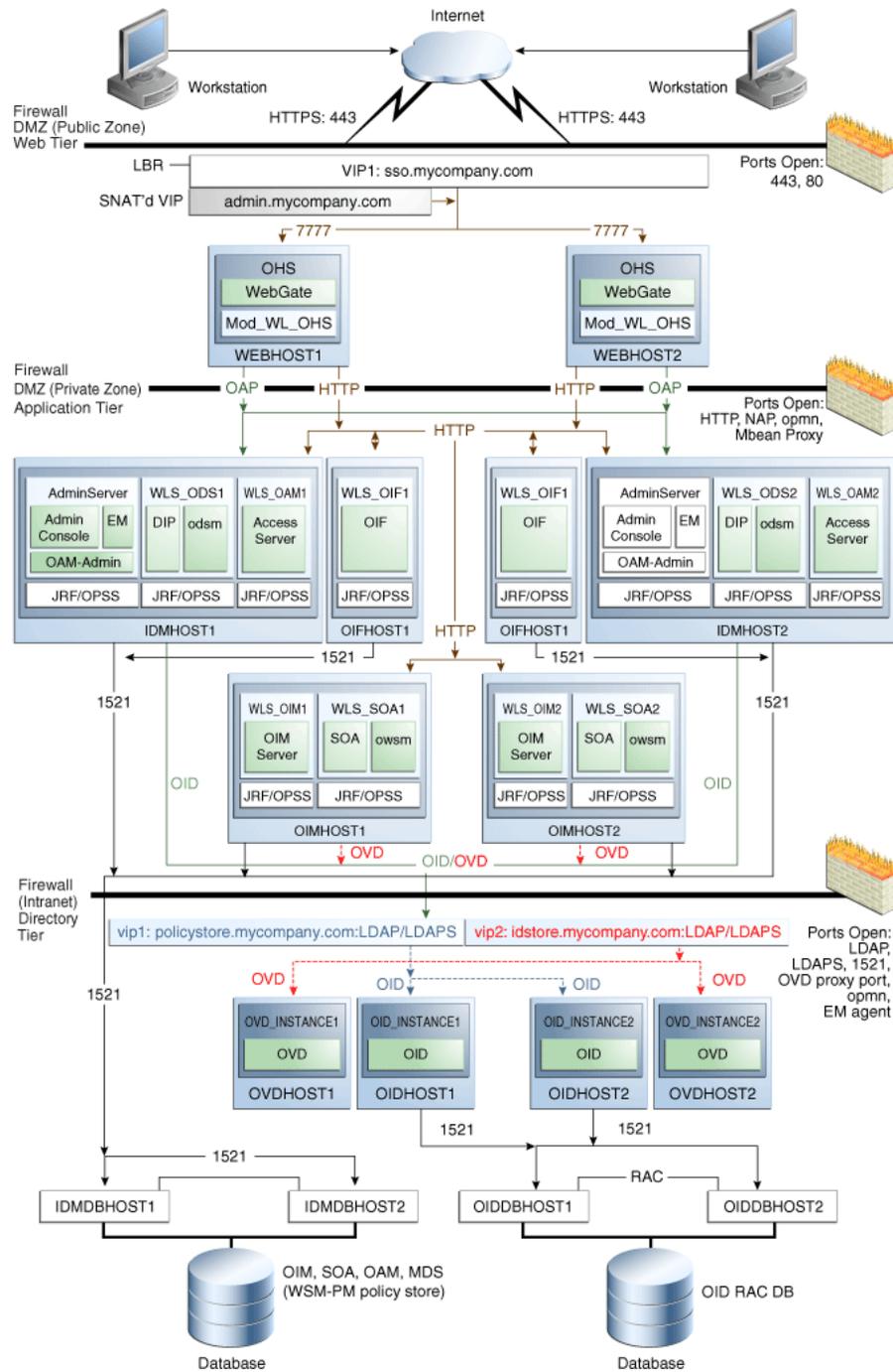
1.5 Understanding the Topology Tiers

The topologies contain three product tiers. This section describes them.

This section contains the following topics:

- Section 1.5.1, "Understanding the Directory Tier"

- Section 1.5.2, "Understanding the Application Tier"

- Section 1.5.3, "Understanding the Web Tier"

1.5.1 Understanding the Directory Tier

The directory tier is in the Intranet Zone. The directory tier is the deployment tier where all the LDAP services reside. This tier includes products such as Oracle Internet Directory and Oracle Virtual Directory. The directory tier is managed by directory administrators providing enterprise LDAP service support.

The directory tier is closely tied with the data tier. Access to the data tier is important for the following reasons:

- Oracle Internet Directory relies on Oracle Database as its back end.

- Oracle Virtual Directory provides virtualization support for other LDAP services or databases or both.

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.

Typically protected by firewalls, applications above the directory tier access LDAP services through a designated LDAP host port. The standard LDAP port is 389 for the non-SSL port and 636 for the SSL port. LDAP services are often used for white pages lookup by clients such as email clients in the intranet.

The directory tier stores two types of information:

- Identity Information–used for storing information about users and groups

- Policy Information–used for storing information about security policies and for configuration information.

You must always store policy information in Oracle Internet Directory. You may store identity information in Oracle Internet Directory or in another directory such as Microsoft Active Directory.

If you store identity information in a non-OID directory, you can either use Oracle Virtual Directory to present that information or use Oracle Directory Integration Platform to synchronize the users and groups from the non-oracle directory to Oracle Internet Directory.

A split directory configuration is one where identity data is stored in multiple directories, possibly in different locations. Use this kind of deployment when you do not want to modify the existing Identity Store by extending the schema. In that case, deploy a new directory, either Oracle Internet Directory or Active Directory, to store the extended attributes. Alternatively, you can use the Policy Store Oracle Internet Directory for this purpose. In this scenario, use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret.

> **See Also:** Chapter 10, "Preparing Directories Other than Oracle Internet Directory" for information about configuring Oracle Virtual Directory in a split directory environment.

Although you can use a single Oracle Internet Directory instance for storing both the identity and policy information, in some cases it might be required that you use two separate Oracle Internet Directory installations - one for the Policy Store and another for Identity Store. Examples include the following scenarios:

- You want to enable Oracle Internet Directory referential integrity for the Identity Store.

- The throughput or enterprise directory requirements dictate separating out the two stores

- You have a shared Identity Management or Multi-tenant Identity Management deployment with multiple Oracle Fusion Applications pods pointing to it.

If you intend to separate your identity and policy information, you must create two separate clusters of highly available Oracle Internet Directory. These Oracle Internet Directory clusters can share the same machines but they should use separate Real Application Clusters databases as their data store.

If you are using Oracle Internet Directory exclusively, you do not need to use Oracle Virtual Directory.

This guide assumes that you are creating two virtual names: one for your Policy Store (`policystore.mycompany.com`) and one for your Identity Store (`idstore.mycompany.com`). When using a single Oracle Internet Directory for both your identity and policy information, you can either create two virtual host names, both pointing to the same directory, or combine them into a single suitable virtual host name in the load balancer.

1.5.2 Understanding the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Manager, Oracle Directory Integration Platform, Oracle Identity Federation, Oracle Directory Services 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 Management applications in the application tier interact with the directory tier as follows:

- In some cases, 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 and Oracle Directory Services Manager are administration tools that provide 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.

In the application tier:

- `IDMHOST1` and `IDMHOST2` have the WebLogic Server with the Administration Console, Oracle Enterprise Manager Fusion Middleware Control, Oracle Directory Integration Platform, Oracle Directory Services Manager and Oracle Access Server installed. `IDMHOST1` and `IDMHOST2` run both the WebLogic Server Administration Servers and Managed Servers. Note that the Administration Server is configured to be active-passive, that is, although it is installed on both nodes, only one instance is active at any time. If the active instance goes down, then the passive instance starts up and becomes the active instance.

  The Oracle Access Server communicates with Oracle Virtual Directory in the directory tier to verify user information.

- On the firewall protecting the application tier, the HTTP ports, and OAP port are open. The OAP (Oracle Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.

- In the OAM and OIM topology, `OIMHOST1` and `OIMHOST2` have Oracle Identity Manager and Oracle SOA installed. Oracle Identity Manager is user provisioning application. Oracle SOA deployed in this topology is exclusively used for providing workflow functionality for Oracle Identity Manager.

- `OIFHOST1` and `OIFHOST2` have the WebLogic Server with Oracle Identity Federation installed.

1.5.2.1 Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Services (OPSS) agent.

- The Administration Server, Oracle Enterprise Manager and Oracle Access Manager console are always bound to the listen address of the Administration Server.

- The `WLS_ODS1` Managed Server on `IDMHOST1` and `WLS_ODS2` Managed Server on `IDMHOST2` are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.

- The `WLS_OAM1` Managed Server on `IDMHOST1` and `WLS_OAM2` Managed Server on `IDMHOST2` are in a cluster and the Access Manager applications are targeted to the cluster.

- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the `WLS_ODS1` and `WLS_ODS2` Managed Servers. By default, the listen address for these Managed Servers is set to `IDMHOST1` and `IDMHOST2` respectively.

- In the OAM + OIM topology, the `WLS_OIM1` Managed Server on `OIMHOST1` and `WLS_OIM2` Managed Server on `OIMHOST2` are in a cluster and the Oracle Identity Manager applications are targeted to the cluster.

- In the OAM + OIM topology, the `WLS_SOA1` Managed Server on `OIMHOST1` and `WLS_SOA2` Managed Server on `OIMHOST2` are in a cluster and the `Oracle` SOA applications are targeted to the cluster

- The `WLS_OIF1` Managed Server on `OIFHOST1` and `WLS_OIF2` Managed Server on `OIFHOST2` are in a cluster and the Oracle Directory Services Manager and Access Manager applications are targeted to the cluster.

1.5.2.2 High Availability Provisions

- The Access Servers are active-active deployments.

- In the Oracle Access Manager and Oracle Identity Manager topology, the Identity Management Servers and SOA Servers 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).

- The Identity Federation Servers are active-active deployments; the Access Server may communicate with the data tier at run time.

- The WebLogic Administration Server is a singleton component deployed in an active-passive configuration. If `IDMHOST1` fails or the Administration Server on

IDMHOST1 does not start, the Administration Server on IDMHOST2 can be started. All Managed Servers and components on IDMHOST1 and IDMHOST2 must be configured with the Administration Server virtual IP address.

1.5.2.3 Security Provisions

Oracle WebLogic Server Console, Oracle Enterprise Manager Fusion Middleware Control console, and Oracle Access Manager console are only accessible through admin.mycompany.com, which is only available inside the firewall.

1.5.3 Understanding 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 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 Oracle Access Manager, the web tier is required.

While components such as Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager 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 Oracle 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 Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on IDMHOST1 and IDMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

On the firewall protecting the web tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.

1.5.3.1 Architecture Notes

Oracle HTTP Servers on WEBHOST1 and WEBHOST2 are configured with mod_wl_ohs, and proxy requests for the Oracle Enterprise Manager, Oracle Directory Integration Platform, and Oracle Directory Services Manager Java EE applications deployed in WebLogic Server on IDMHOST1 and IDMHOST2.

1.5.3.2 Security Provisions

The Oracle HTTP Servers process requests received using the URL's sso.mycompany.com and admin.mycompany.com. The nameadmin.mycompany.com is only resolvable inside the firewall. This prevents access to sensitive resources such as the Oracle WebLogic Server console and Oracle Enterprise Manager Fusion Middleware Control console from the public domain.

1.6 Using This Guide

Follow these steps to install the software and extend your domain with the components required in your environment.

1. Read the current chapter, Chapter 1, "Enterprise Deployment Overview."

2. Ensure that you have performed all prerequisite steps, as described in Chapter 2, "Prerequisites for Enterprise Deployments."

3. Configure the database repository, as described in Chapter 3, "Configuring the Database Repositories."

4. Install the software, as described in Chapter 4, "Installing the Software."

5. Configure the Web Tier, as described in Chapter 5, "Configuring the Web Tier."

6. Create the WebLogic domain, as described in Chapter 6, "Creating the WebLogic Server Domain for Identity Management."

7. Extend the domain with Oracle Internet Directory, as described in Chapter 7, "Extending the Domain with Oracle Internet Directory."

8. Extend the domain with Oracle Directory Integration Platform (optional) and ODSM, as described in Chapter 8, "Extending the Domain with Oracle Directory Integration Platform and ODSM."

9. If you intend to store your identity data in a directory other than Oracle Internet Directory or in a split directory, perform the procedures described in Chapter 9, "Extending the Domain with Oracle Virtual Directory" and Chapter 10, "Preparing Directories Other than Oracle Internet Directory." If your Identity Store includes only Oracle Internet Directory, skip this step.

10. Prepare the Identity and Policy Stores. See Section 11, "Preparing Identity and Policy Stores."

11. Extend the domain with Oracle Access Manager. See Section 1, "Enterprise Deployment Overview."

12. Extend the domain with Oracle Identity Manager as described in Section 12, "Extending the Domain with Oracle Access Manager 11g."

13. If you are using Oracle Identity Federation, follow the steps in Section 14, "Extending the Domain with Oracle Identity Federation." Otherwise, skip this step.

14. Set up Node Manager. See Section 15, "Setting Up Node Manager."

15. Configure server migration for Oracle Identity Manager, as described in Section 16, "Configuring Server Migration for Oracle Identity Manager."

16. Integrate components as described in Section 17, "Integrating Components."

17. Configure single sign-on for administration modules. See Section 18, "Configuring Single Sign-on for Administration Consoles."

2

Prerequisites for Enterprise Deployments

This chapter describes the prerequisites for the Oracle Identity Management Infrastructure enterprise deployment topologies.

This chapter includes the following topics:

- Section 2.1, "Hardware Resource Planning"
- Section 2.2, "Network Prerequisites"
- Section 2.3, "WebLogic Domain Considerations"
- Section 2.4, "Shared Storage and Recommended Directory Structure"

2.1 Hardware Resource Planning

The minimum hardware requirements for the Enterprise Deployment on Linux operating systems are listed in Table 2–1. The memory figures represent the memory required to install and run an Oracle Fusion Middleware server; however, for most production sites, you should configure at least 4 GB of physical memory.

For detailed requirements, or for requirements for other platforms, see the *Oracle Fusion Middleware Installation Guide* for that platform.

Table 2–1   Typical Hardware Requirements

Server	Processor	Disk	Memory	TMP Directory	Swap
Database Hosts (OIDDBHOST*n*, OIDDBHOST*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
IDMHOST*n*, OAMHOST*n*, OIMHOST*n*	2 or more X Pentium 1.5 GHz or greater	10 GB	6 GB	Default	Default
OIDHOST*n*, OVDHOST*n*	2 or more X Pentium 1.5 GHz or greater	10 GB	4 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; however, this 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 servers to the configuration by repeating the instructions for the second server (that is, WEBHOST2, IDMHOST2, OIDHOST2, OVDHOST2, OIDDBHOST2) to install and configure additional servers where needed.

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

2.2 Network Prerequisites

This section describes the network prerequisites for the enterprise deployment topologies:

- Load balancers
- Configuring virtual server names and ports on the load balancer
- Administration Server Virtual IP Addresses
- Managing Oracle Fusion Middleware component connections
- Oracle Access Manager communication protocols and terminology
- Firewall and port configuration

This section contains the following topics:

- Section 2.2.1, "Load Balancers"
- Section 2.2.2, "Configuring Virtual Server Names and Ports on the Load Balancer"
- Section 2.2.3, "Virtual IP Addresses"
- Section 2.2.4, "Managing Oracle Fusion Middleware Component Connections"
- Section 2.2.5, "Oracle Access Manager Communication Protocol and Terminology"
- Section 2.2.6, "Firewall and Port Configuration"

2.2.1 Load Balancers

The enterprise topologies use 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 host name: Clients access services using the virtual host name (instead of using actual host 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 OracleAS 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.

- 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.

- Sticky routing capability: Ability to maintain sticky connections to components based on cookies or URL.

- SSL acceleration (this feature is recommended, but not required).

- Configure the virtual server(s) in the load balancer for the directory tier with a high value for the connection timeout for TCP connections. This value should be more than the maximum expected time over which no traffic is expected between the Oracle Access Manager and the directory tier.

- 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.

2.2.2 Configuring Virtual Server Names and Ports on the Load Balancer

Several 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 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.

There are two load balancer devices in the recommended topologies. 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 DMZs. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant

mode. The rest of this document assumes that the deployment is one of those shown in Chapter 1.

policystore.mycompany.com

- This virtual server is enabled on `LBR2`. It acts as the access point for all policy-based LDAP traffic, which is stored in the Oracle Internet Directory servers in the directory tier. Traffic to both the SSL and non-SSL is configured. The clients access this service using the address `policystore.mycompany.com:636` for SSL and `policystore.mycompany.com:389` for non-SSL.

  > **Note:** Oracle recommends that you configure the same port for SSL connections on the LDAP server and Oracle Internet Directory on the computers on which Oracle Internet Directory is installed.
  >
  > This is a requirement for most Oracle 10*g* products that use Oracle Internet Directory through the load balancing router.

- Monitor the heartbeat of the Oracle Internet Directory processes on `OIDHOST1` and `OIDHOST2`. If an Oracle Internet Directory process stops on `OIDHOST1` or `OIDHOST2`, or if either host `OIDHOST1` or `OIDHOST2` is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

idstore.mycompany.com

- This virtual server is enabled on `LBR2`. It 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.

- If your identity store is accessed through Oracle Virtual Directory, monitor the heartbeat of the Oracle Virtual Directory processes on `OVDHOST1` and `OVDHOST2`. If an Oracle Virtual Directory process stops on `OVDHOST1` or `OVDHOST2`, or if either host `OVDHOST1` or `OVDHOST2` is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

- If your identity store is in Oracle Internet Directory and is accessed directly, monitor the heartbeat of the Oracle Internet Directory processes on the Oracle Internet Directory Hosts. If an Oracle Internet Directory process stops on one `OIDHOST` or one `OIDHOST` is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

admin.mycompany.com

- This virtual server is enabled on `LBR1`. It acts as the access point for all internal HTTP traffic that gets directed to the administration services. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `admin.mycompany.com:80` and in turn forward these to ports 7777 on `WEBHOST1` and `WEBHOST2`. The services accessed on this virtual host include the WebLogic Administration Server Console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Directory Services Manager.

- Create rules in the firewall to block outside traffic from accessing the `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `admin.mycompany.com` virtual host.

oiminternal.mycompany.com

- This virtual server is enabled on LBR1. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `oiminternal.mycompany.com:80` and in turn forward these to ports `7777` 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 `oiminternal.mycompany.com` virtual host.

sso.mycompany.com

- This virtual server is enabled on `LBR1`. It 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 ports 7777 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 and port 443.

- 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.

In addition, 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.

2.2.3 Virtual IP Addresses

adminvhn.mycompany.com

In enterprise deployments, the Administration Server must be able to continue processing requests after a host it is residing on fails. In Enterprise deployments the 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 `IDMHOST1` to `IDMSHOST2`, or vice versa.

soavhnx

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.

oimvhnx

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.

2.2.4 Managing Oracle Fusion Middleware Component Connections

To ensure consistent availability of all services, ensure that the connection timeout values for all Oracle Fusion Middleware components are set to a lower timeout value than that on the firewall and load balancing router. If the firewall or load balancing router drops a connection without sending a TCP close notification message, then Oracle Fusion Middleware components continue to try to use the connection when it is no longer available.

2.2.5 Oracle Access Manager Communication Protocol and Terminology

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

2.2.5.1 Oracle Access Manager Protocols

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

2.2.5.2 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 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 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 Server over Oracle Access Protocol and the Access 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.

2.2.6 Firewall and Port Configuration

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 during installation.

Table 2–2 lists the ports used in the Oracle Identity Management topologies, including the ports that you must open on the firewalls in the topologies.

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 directory tier.

Table 2–2   Ports Used in the Oracle Identity Management Enterprise Deployment topologies

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 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 Management.
Oracle WebLogic Administration Server access from web tier	FW1	7001	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_ODS`	FW1	7006	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the `mod_weblogic` parameters used.
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 Process Manager and Notification Server (OPMN) access in web tier	FW1	OPMN remote port	HTTP / Administration Server to OPMN	Outbound	N/A
Oracle HTTP Server proxy port	FW1	9999	HTTP / Administration Server to Oracle HTTP Server	Outbound	N/A
Access Server 10*g* access	FW1	6021	OAP	Both	N/A
Access Server 11*g*	FW1	5574-5575	OAP	Both	N/A
Oracle Coherence Port	FW1	8000 - 8090	TCMP	Both	N/A
Oracle WebLogic Administration Server access from directory tier	FW2	7001	HTTP / Oracle Internet Directory, Oracle Virtual Directory, and Administration Server	Outbound	N/A

Table 2–2 (Cont.) Ports Used in the Oracle Identity Management Enterprise Deployment topologies

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Enterprise Manager Agent - directory tier to Enterprise Manager	FW2	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
OPMN access in directory tier	FW2	OPMN remote port	HTTP / Administration Server to OPMN	Inbound	N/A
Oracle Virtual Directory proxy port	FW2	8899	HTTP / Administration Server to Oracle Virtual Directory	Inbound	N/A
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Identity Management.
Oracle Internet Directory access	FW2	389	LDAP	Inbound	Tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Internet Directory access	FW2	636	LDAP SSL	Inbound	Tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	6501	LDAP	Inbound	Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	7501	LDAP SSL	Inbound	Ideally, these connections should be configured not to time out.
Oracle Identity Federation access	FW2	7499	HTTP	Both	N/A
APM	FW2	7001	HTTP	Both	N/A
OIN	FW2	7001	HTTP	Both	N/A
Load balancer to Oracle HTTP Server	N/A	7777	HTTP	N/A	N/A
Session replication within a WebLogic Server cluster	N/A	N/A	N/A	N/A	By default, this communication uses the same port as the server's listen address.
Node Manager	N/A	5556	TCP/IP	N/A	N/A

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

2.3 WebLogic Domain Considerations

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 context of Identity Management, it is recommended that the Identity Management components be deployed in a separate WebLogic Server domain from SOA, WebCenter and other customer applications that might be deployed. In a typical enterprise deployment, the administration of identity management components such as LDAP directory, single sign-on solutions, and provisioning solutions is done by a different set of administrators from those who administer the middleware infrastructure and applications.

It is technically possible to deploy everything in a single domain in a development or test environment. However, in a production environment, the recommendation to use separate domains creates a logical administrative boundary between the identity management stack and the rest of the middleware and application deployment.

2.4 Shared Storage and Recommended Directory Structure

This section details the directories and directory structure that Oracle recommends for an EDG topology. 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.

This section contains the following topics:

- Section 2.4.1, "Directory Structure Terminology and Environment Variables"

- Section 2.4.2, "Recommended Locations for the Different Directories"

2.4.1 Directory Structure Terminology and Environment Variables

This section describes directory structure terminology and environment variables.

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

- MW_HOME: This environment 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.

- WL_HOME: This environment variable and related directory path contains installed files necessary to host a WebLogic Server.

- ORACLE_HOME: This environment variable points to the location where an Oracle Fusion Middleware product, such as Oracle HTTP Server, Oracle SOA

Suite, or Oracle Internet Directory is installed and the binaries of that product are being used in a current procedure

- ORACLE_COMMON_HOME: This environment variable and related directory path refers to the location where the Oracle Fusion Middleware Common Java Required Files (JRF) Libraries and Oracle Fusion Middleware Enterprise Manager Libraries are installed.

- Domain directory: This path refers to the file system location where the Oracle WebLogic domain information (configuration artifacts) is stored. Different WebLogic Servers can use different domain directories even when in the same node as described Section 2.4.2, "Recommended Locations for the Different Directories."

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

2.4.2 Recommended Locations for the Different Directories

Oracle Fusion Middleware 11*g* allows the separation of the product binaries and the run-time artifacts.

In this enterprise deployment model, for the web tier and the data tier, it is recommended to have one `ORACLE_HOME` (for product binaries) per host and one `ORACLE_INSTANCE` for an instance, installed on the local or shared disk. The `ORACLE_HOME` can be shared by all the instances running on the host. Each instance has its own `ORACLE_INSTANCE` location. Both `ORACLE_HOME` and `ORACLE_INSTANCE` can also be located on a shared disk mounted to the respective boxes. Additional servers (when scaling out or up) of the same type can use one of these `MW_HOME` without requiring more installations.

For the application tier, it is recommended to have Middleware Home (`MW_HOME`) on a shared disk. It is recommended to have two `MW_HOME` in the domain for High Availability. An application Tier node mounts either one of these on a mount point. This mount point should be the same on all the application tier nodes. Additional servers (when scaling out or up) of the same type can use one of these `MW_HOME`s without requiring more installations.

Based on these recommendations, Table 2–3 lists the recommended directory structure. The directory locations listed are examples and can be changed. However, Oracle recommends that these locations be used for uniformity, consistency and simplicity.

Note:

- In the following table, wherever shared storage is required for a directory, the shared storage column specification is qualified with the word Yes. When using local disk or shared storage is optional, the shared storage column specification is qualified with the word Optional. The shared storage locations are examples and can be changed as long as the provided mount points are used.

- When you're installing a high availability topology across multiple homes, Oracle recommends using the same directory structure for all nodes.

Table 2–3   Recommended Directory Structure

	Environment Variable	Mount Point or Directory Structure	Shared Storage Location	Host Name	Shared Storage
Common	ORACLE_BASE	/u01/app/oracle			
	MW_HOME	*ORACLE_BASE*/product/fmw			
	JAVA_HOME	*MW_HOME*/jrockit_*version*			
	ORACLE_ COMMON_HOME	*MW_HOME*/oracle_common			
Web Tier	WEB_ORACLE_ HOME	*MW_HOME*/web			Optional
	ORACLE_ INSTANCE	*ORACLE_ BASE*/admin/*instanceName*			Optional
Identity Management Application Tier	MW_HOME	*ORACLE_BASE*/*product*/fmw	/vol/*MW_HOME1*	IDMHOST1 OIMHOST1 OIFHOST1	Yes
	MW_HOME	*ORACLE_BASE*/*product*/fmw	/vol/*MW_HOME2*	IDMHOST2 OIMHOST2 OIFHOST2	Yes
	IDM_ORACLE_ HOME	*MW_HOME*/idm			Yes
	IAM_ORACLE_ HOME	*MW_HOME*/iam			
	SOA_ORACLE_ HOME	*MW_HOME*/soa			
	WL_HOME	*MW_HOME*/wlserver_*version*			Yes
	ORACLE_ INSTANCE	*ORACLE_ BASE*/admin/*instanceName*			Optional
	ASERVER_HOME	*ORACLE_ BASE*/admin/*domainName*/aserver	/vol/admin	IDMHOST1	Yes
	ASERVER_ DOMAIN_HOME	*ASERVER_HOME*/*domainName*			
	ASERVER_APP_ HOME	*ASERVER_HOME*/applications			
	MSERVER_HOME	*ORACLE_ BASE*/admin/*domainName*/mserver			Optional
	MSERVER_ DOMAIN_HOME	*MSERVER_HOME*/*domainName*			
	MSERVER_APP_ HOME	*MSERVER_HOME*/applications			
OAM 10*g* Application Tier	OAM_BASE	*MW_HOME*/oam			Optional
	IDENTITY_ SERVER_ ORACLE_HOME	*OAM_BASE*/identity			Optional
	ACCESS_ SERVER_ ORACLE_HOME	*OAM_BASE*/access			Optional

Table 2–3   (Cont.) Recommended Directory Structure

	Environment Variable	Mount Point or Directory Structure	Shared Storage Location	Host Name	Shared Storage
	WEBPASS_ ORACLE_HOME	*OAM_ BASE*/webcomponents/identity			Optional
	POLICY_ MANAGER_ ORACLE_HOME	*OAM_BASE*/webcomponents/access			Optional
	WEBGATE_ ORACLE_HOME	*OAM_BASE*/webgate			Optional
Directory Tier	IDM_ORACLE_ HOME	*MW_HOME*/idm			Optional
	ORACLE_ INSTANCE	*ORACLE_ BASE*/admin/*instanceName*			Optional

The following commands are examples. Use the appropriate commands for your Operating System.

- To mount the MW_HOME1 volume on the shared storage to the MW_HOME mountpoint on IDMHOST1 run the following command on IDMHOST1 as root:

```
mount storageHost:/Path_to_MW_HOME1_volume_on_SharedDisk
MW_HOME_moutpoint_on_IDMHOST1
-t nfs
-o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

For Example:

```
mount storageHost:/vol/MW_HOME1 /u01/app/oracle/product/fmw -t nfs \
    -o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

- To mount the MW_HOME2 volume on the shared storage to the MW_HOME mountpoint on IDMHOST2 run the following command on IDMHOST2 as root:

```
mount storageHost:/Path_to_MW_HOME2_volume_on_SharedDisk \
MW_HOME_moutpoint_on_IDMHOST2 -t nfs \
-o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

For Example:

```
mount storageHost:/vol/MW_HOME2 /u01/app/oracle/product/fmw -t nfs \
    -o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

- To mount the ADMIN volume on the shared storage to the AServer_Home mountpoint on IDMHOST1 run the following command on IDMHOST1 as root:

```
mount storageHost:/Path_to_ADMIN_volume_on_SharedDisk \
ASERVER_HOME_moutpoint_on_IDMHOST1 -t nfs \
-o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

For Example:

```
mount storageHost:/vol/ADMIN /u01/app/oracle/admin/IDMDomain/aserver -t nfs \
    -o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768
```

Figure 2–1 shows the recommended directory structure.

Figure 2–1   Directory Structure for Identity Management
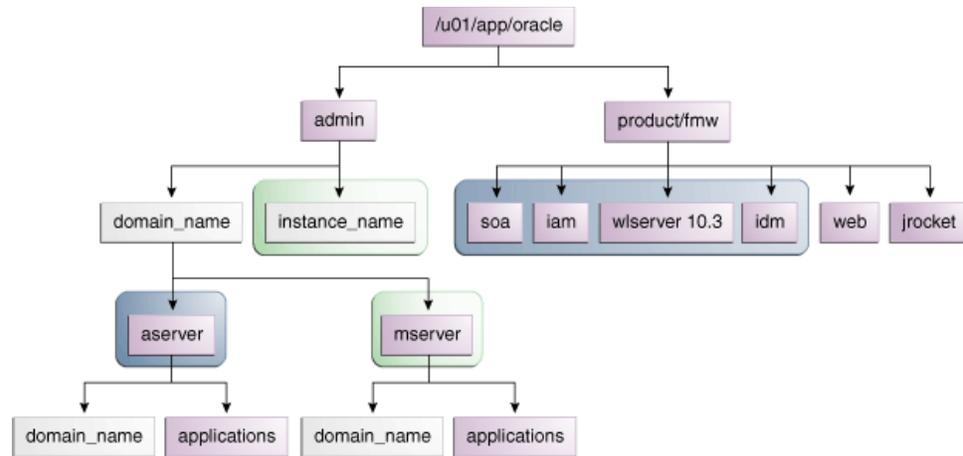
Table 2–4 explains what the color-coded elements in Figure 2–1 mean. The directory structure in Figure 2–1 does not show other required internal directories such as ORACLE_COMMON_HOME and jrockit.

Table 2–4   Directory Structure Elements

Element	Explanation
	The Administration Server domain directories, applications, deployment plans, file adapter control directory, JMS and TX logs, and the entire MW_ HOME are on a shared disk.
	The Managed Server domain directories can be on a local disk or a shared disk. Further, if you want to share the Managed Server domain directories on multiple nodes, then you must mount the same shared disk location across the nodes. The instance_name directory for the web tier can be on a local disk or a shared disk.
	Fixed name.
	Installation-dependent name.

3

Configuring the Database Repositories

This chapter describes how to install and configure the database repositories. It contains the following topics:

- Section 3.1, "Real Application Clusters"
- Section 3.2, "Configuring the Database for Oracle Fusion Middleware 11g Metadata"
- Section 3.3, "Executing the Repository Creation Utility"

Before beginning to install and configure the Identity Management components, you must perform the following steps:

- Install and configure the Oracle database repositories. See the installation guides listed in the "Related Documents" section of the Preface and Section 3.2, "Configuring the Database for Oracle Fusion Middleware 11g Metadata."
- Create the required Oracle schemas in the database using the Repository Creation Utility (RCU). See Section 3.3, "Executing the Repository Creation Utility."

Databases Required

For Oracle Identity management, a number of separate databases are recommended. A summary of these databases is provided in Table 3–1. Which database or databases you use is dependent on the topology that you are implementing:

Table 3–1   Mapping between Topologies, Databases and Schemas

Topology Type	Database Names	Database Hosts	Service Names	Schemas in Database
Oracle Access Manager 11*g* and Oracle Identity Manager 11*g* (`OAM11g/OIM11g`)	`OIDDB`	`OIDDBHOST1` `OIDDBHOST2`	`oidedg.mycom` `pany.com`	`ODS`,
	`IDMDB`	`IDMDBHOST1` `IDMDBHOST2`	`oamedg.mycom` `pany.com` `oimedg.mycom` `pany.com`	`OAM`, `IAU`, `ORASDPM`, `MDS`[1], `OIM`, `SOAINFRA`
Oracle Identity Federation 11*g* (`OIF11g/OAM11g`)	`OIDDB`	`OIDDBHOST1` `OIDDBHOST2`	`oidedg.mycom` `pany.com`	`ODS`

Table 3–1   (Cont.) Mapping between Topologies, Databases and Schemas

Topology Type	Database Names	Database Hosts	Service Names	Schemas in Database
	IDMDB	IDMDBHOST1 IDMDBHOST2	oamedg.mycom pany.com oimedg.mycom pany.com oifedg.mycom pany.com	OAM, IAU, ORASDPM, MDS, OIM, SOAINFRA, OIF

[1] The SOA and Oracle Identity Manager components share the MDS repository.

> **Notes:**   If you are using Oracle Internet Directory to store both your identity and policy information, and separating this information across two Oracle Internet Directory instances, then two databases are required for the ODS schema.

The following sections apply to all the databases listed in Table 3–1.

Database Versions Supported

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/fusio n-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%';
```

3.1 Real Application Clusters

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 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.

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*.

3.2 Configuring the Database for Oracle Fusion Middleware 11*g* Metadata

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

- Section 3.2.1, "Creating a Real Applications Clusters Database"

- Section 3.2.2, "Creating Database Services for 10.x and 11.1.x Databases"

- Section 3.2.3, "Creating Database Services for 11.2.x Databases"

- Section 3.2.4, "Database Tuning"

3.2.1 Creating a Real Applications 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.

- In addition the database must have the following minimum initialization parameters defined:

Table 3–2   Minimum Initialization Parameters for Oracle RAC Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	800[1]
session_max_open_ files	50

Table 3–2   (Cont.) Minimum Initialization Parameters for Oracle RAC Databases

Parameter	Value
sessions	500
processes	500
sga_target	512M
sga_max_size	800M
pga_aggregate_target	100M
session_cached_ cursors	500
processes	2500
sga_target	4G
pga_aggregate_target	2G

[1]   OAM requires a minimum of 800 open cursors in the database. When OIM and OAM are available, the number of open cursors should be 1500.

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

Oracle recommends using the Oracle Enterprise Manager Cluster Managed Services page to create database services that client applications use to connect to the database. 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

1.   Log on to SQL*Plus as the sysdba user and run the following command to create a service called oamedg.mycompany.com for Oracle Access Manager:

```
SQL> 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:

```
prompt> srvctl add service -d oamadb -s oamedg.mycompany.com -r idmdb1,idmdb2
```

3.   Start the service using srvctl:

```
prompt> srvctl start service -d idmdb -s oamedg.mycompany.com
```

When creating a service in the database for Oracle Internet Directory, ensure that the service is enabled for high-availability notifications and configured with the proper server-side Transparent Application Failover (TAF) settings. Use the DBMS_SERVICE package to create the service to enable high availability notification to be sent through Advanced Queuing (AQ) by setting the AQ_HA_NOTIFICATIONS attribute to TRUE and configure server-side Transparent Application Failover (TAF) settings, as follows:

1.   Use the CREATE_SERVICE subprogram to both create the database service and enable high-availability notification and configure server-side Transparent Application Failover (TAF) settings:

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

SQL> EXECUTE
DBMS_SERVICE.CREATE_SERVICE(
SERVICE_NAME => 'oidedg.mycompany.com',
NETWORK_NAME => 'oidedg.mycompany.com',
AQ_HA_NOTIFICATIONS => TRUE,
FAILOVER_METHOD => DBMS_SERVICE.FAILOVER_METHOD_BASIC,
FAILOVER_TYPE => DBMS_SERVICE.FAILOVER_TYPE_SELECT,
FAILOVER_RETRIES => 5, FAILOVER_DELAY => 5);
```

> **Note:** The EXECUTE DBMS_SERVICE command shown must be entered on a single line to execute properly.
>
> For more information about the DBMS_SERVICE package, see the *Oracle Database PL/SQL Packages and Types Reference*.

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

```
prompt> srvctl add service -d oiddb -s oidedg.mycompany.com -r oiddb1,oiddb2
```

3. Start the service using srvctl:

```
prompt> srvctl start service -d oiddb -s oidedg.mycompany.com
```

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

3.2.3 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 3–1, " Mapping between Topologies, Databases and Schemas".

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

```
srvctl add service -d idmdb -s oidedg.mycompany.com -r idmdb1,idmdb2 -q TRUE -m
BASIC -e SELECT -w 5 -z 5
```

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)

> **Note:** Transparent Application Failover (TAF) settings are only required when creating a service for Oracle Internet Directory.

2. Start the Service using `srvctl start service`

   ```
   srvctl start service -d idmdb -s oidedg.mycompany.com
   ```

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

   ```
   srvctl status service -d idmdb -s oidedg.mycompany.com
   Service oidedg.mycompany.com is running on instance(s) idmdb1,idmdb2
   ```

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

   ```
   srvctl config service -d idmdb -s oidedg.mycompany.com
   Service name: oidedg.mycompany.com
   Service is enabled
   Server pool: oiddb_oidedg.mycompany.com
   Cardinality: 2
   Disconnect: false
   Service role: PRIMARY
   Management policy: AUTOMATIC
   DTP transaction: false
   AQ HA notifications: true
   Failover type: SELECT
   Failover method: BASIC
   TAF failover retries: 5
   TAF failover delay: 5
   Connection Load Balancing Goal: LONG
   Runtime Load Balancing Goal: NONE
   TAF policy specification: NONE
   Edition:
   Preferred instances: idmdb1,idmdb2
   Available instances:
   ```

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

3.2.4 Database Tuning

The database parameters defined in Section 3.2.1, "Creating a Real Applications Clusters Database" 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 the following SQL*Plus command:

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

3.3 Executing the Repository Creation Utility

You run RCU to create the collection of schemas used by Identity Management and Management Services.

This section contains the following topics:

1. Section 3.3.1, "Procedure for Executing RCU"

2. Section 3.3.2, "RCU Example"

3.3.1 Procedure for Executing RCU

1. Start RCU by issuing this command:

   ```
   prompt> 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 one of the Oracle RAC nodes. Specify the Virtual IP name. For example: `oiddbhost1-vip.mycompany.com`.

   - **Port:** The port number for the database listener. For example: `1521`

   - **Service Name:** The service name of the database. For example `oidedg.mycompany.com`

   - **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 except for the ODS schema are required to have a prefix For example, enter `EDG`.

   Components: The components specified here depend on the topology being installed. Select the appropriate schemas.

   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 3–1 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. Oracle recommends choosing different passwords for
   different schema's to enhance security

   Click **Next**.

9. On the Map Tablespaces screen, accept the defaults and click **Next**.

10. On the Create Tablespaces 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.

3.3.2 RCU Example

This example illustrates the steps to create the required schemas in the OIDDB and
OIMDB databases for the topology with OAM11*g* and OIM11*g*.

1. Start RCU as described in Section 3.3.1, "Procedure for Executing RCU."

2. On the Welcome Screen, click **Next**.

3. On the Connection Details screen, provide the details to connect to the OIDDB
   database running on OIDDBHOST1 and OIDDBHOST2. Enter the following values:

   - Host: oiddbhost1-vip.mycompany.com

   - Port: 1521

   - Service Name: oidedg.mycompany.com

   - Username: sys

   - Password: *password*

   - Role: SYSDBA

   Click **Next**.

4. On the Select Components screen, select the appropriate schemas by referring to Section 3–1, " Mapping between Topologies, Databases and Schemas."

Click **Next**.

5. Follow the remaining steps in Section 3–1, " Mapping between Topologies, Databases and Schemas" to create the schemas.

6. Verify that the schemas for the `OIDDB` database were successfully created.

7. Start RCU again to create the schemas for the `OIMDB` database.

8. On the Connection Details screen, provide the details to connect to the `OIMDB` database running on `IDMDBHOST1` and `IDMDBHOST2`. Enter the following values:

- Host: `idmdbhost1-vip.mycompany.com`

- Port: `1521`

- Service Name: `oimedg.mycompany.com`

- Username: `sys`

- Password: `password`

- Role: `SYSDBA`

Click **Next**.

9. On the Select Components screen, select the appropriate schemas by referring to Section 3–1, " Mapping between Topologies, Databases and Schemas."

10. Complete the schema creation by following the remaining steps in Section 3.3.1, "Procedure for Executing RCU."

4

Installing the Software

This chapter contains the following topics:

- Section 4.1, "Introduction"
- Section 4.2, "Using this Guide"
- Section 4.3, "Software Installation Summary"
- Section 4.4, "Installing Oracle HTTP Server"
- Section 4.5, "Installing Oracle Fusion Middleware"
- Section 4.6, "Patching the Software"
- Section 4.7, "Backing Up the Installation"

4.1 Introduction

This chapter describes the software installations required for Oracle Identity Management. The installation is divided in two sections. In the first one, the WebTier required installations are addressed. In the second, the required Oracle Fusion Middleware components are installed. Later chapters describe the configuration steps to create the Oracle Identity Management topology.

4.2 Using this Guide

Different topologies use different servers. Before moving on to the detail of creating your topology, you must install the Oracle Software onto the hosts in your topology.

Table 4–1, " Software Versions Used" shows, for each topology, which software should be installed into each host.

The subsequent sections explain how to do this.

> **Note:** Each topology requires the same software to be installed at least twice on two different servers. To achieve this, follow the instructions for installing the appropriate software on each of the servers concerned.

Where two different pieces of Oracle binary software are installed onto the same host (for example OIM11g and OAM11g), this software is installed in the same Middleware home location, but in different Oracle homes.

All software uses the same Middleware home location.

> **Notes:**
>
> - If you are using shared storage, ensure that users and groups used in the installation have the same ID on all hosts that use the storage. If you fail to do this, some hosts might not be able to see or execute some all the files.
>
> - Some products, such as Oracle Internet Directory and Oracle Virtual Directory, require you to run a script that sets the permissions of some files to `root`.

Table 4–1   Software Versions Used

Abbreviation	Product	Version
OHS11G	Oracle HTTP Server	11.1.1.5.0
JRockit	Oracle JRockit	jrockit_160_24_D1.1.2-4
WLS	Oracle WebLogic Server	10.3.5.0
IAM	Oracle Identity and Access Management	11.1.1.5.0
SOA	Oracle SOA Suite	11.1.1.5.0
IDM	Oracle Identity Management	11.1.1.5.0

4.3 Software Installation Summary

Different topologies require different software to be installed. The installation process is the same for each product. Install the software shown in Table 4–1, " Software Versions Used" and Table 4–2, " Software to be Installed for Different Topologies" for the desired topology, according to the instructions in this chapter

Table 4–2   Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	WLS	IAM	SOA	IDM
All	WEBHOST1	X				
	WEBHOST2	X				
OAM11g/OIM11g	IDMHOST1		X	X	X	X
	IDMHOST2		X	X	X	X
	OIMHOST1		X	X	X	X
	OIMHOST2		X	X	X	X
	OIDHOST1					X
	OIDHOST2					X
	OVDHOST1					X

Table 4–2   (Cont.) Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	WLS	IAM	SOA	IDM
	OVDHOST2					X
OIF11g/OAM11g	IDMHOST1		X	X	X	X
	IDMHOST2		X	X	X	X
	OIFHOST1		X	X	X	X
	OIFHOST2		X	X	X	X
	OIDHOST1					X
	OIDHOST2					X
	OVDHOST1					X
	OVDHOST2					X

Oracle Identity Management products are bundled as two product sets: Oracle Identity Management and Oracle Identity and Access Management.(see Table 4–1, " Software Versions Used".) The relevant Identity Management software is installed into separate Oracle homes.

4.4 Installing Oracle HTTP Server

This section explains how to install Oracle HTTP Server on WEBHOST1 and WEBHOST2 (Enterprise Deployments only).

This section contains the following topics:

- Section 4.4.1, "Prerequisites"
- Section 4.4.2, "Installation"
- Section 4.4.3, "Upgrading Oracle HTTP Server from 11.1.1.2 to 11.1.1.5"

4.4.1 Prerequisites

Prior to installing the Oracle HTTP server, check that your machines meet the following requirements:

1. Ensure that the system, patch, kernel, and other requirements are met as specified in *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

2. Ensure that port 7777 is not in use, as described in Section 4.4.1.1.

3. On Linux platforms, if the /etc/oraInst.loc file exists, check that its contents are correct, as described in Section 4.4.1.2.

4.4.1.1 Check Port 7777

Because Oracle HTTP Server is installed by default on port 7777, you must ensure that port 7777 is not used by any other service on the nodes. To check if this port is in use, run the following command before installing Oracle HTTP Server. You must free the port if it is in use.

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

4.4.1.2 Check oraInst.loc

Check that the inventory directory is correct and that you have write permissions for that directory. If the `/etc/oraInst.loc` file does not exist, you can skip this step.

The contents of the `oraInst.loc` file are shown in this example:

```
inventory_loc=/u01/app/oraInventory
inst_group=oinstall
```

4.4.2 Installation

As described in Section 2.4, "Shared Storage and Recommended Directory Structure," you install the Oracle HTTP Server onto a local disk. You can install it on shared storage, but if you do that, you must allow access from the Web Tier DMZ to your shared disk array, which is undesirable. If you decide to install onto shared disk then please see the Release Notes for further configuration information.

Start the Oracle Universal Installer as follows:

On UNIX, issue the command

```
runInstaller
```

On Windows, double-click `setup.exe`.

Before Starting the install, ensure that the following environment variables are not set on UNIX and Linux platforms.

- `LD_ASSUME_KERNEL`
- `ORACLE_INSTANCE`

On the Specify Inventory Directory screen, do the following:

- Enter *HOME*/`oraInventory`, where HOME is the home directory of the user performing the installation (this is the recommended location).
- Enter the OS group for the user performing the installation.
- Click **Next**.

Follow the instructions on screen to execute `createCentralInventory.sh` as `root`.

Click **OK**.

Proceed as follows:

1. On the Specify Oracle Inventory Directory screen, enter *HOME*/`oraInventory`, where `HOME` is the home directory of the user performing the installation. (This is the recommended location).

   Enter the OS group for the user performing the installation.

   Click **Next**.

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

3. On the Select Installation Type screen, select **Install–Do Not Configure**

   Click **Next**.

4. On the Prerequisite Checks screen, click **Next**.

5. On the Specify Installation Location screen, specify the following values:

- **Fusion Middleware Home Location (Installation Location)** For example:

  `/u01/app/oracle/product/fmw`

- **Oracle Home Location Directory**: `web`

6. On the Specify SecurityUpdates screen, choose whether to receive security updates from 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), and click **Install**.

4.4.3 Upgrading Oracle HTTP Server from 11.1.1.2 to 11.1.1.5

Follow these steps to upgrade the Oracle HTTP Server from 11.1.1.2 to 11.1.1.5 on `WEBHOST1` and `WEBHOST2`:

1. Start the WebTier Patchset Installer by running `./runInstaller`.

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

3. On the Specify Install Location screen, provide the path to the Oracle Middleware home and the name of the Oracle home directory.

- **Oracle Middleware Home**: Select the previously installed Middleware Home from the list, for example: `/u01/app/oracle/product/fmw`

- **Oracle Home Directory**: Enter `web` as the Oracle home directory. This Oracle home contains the Oracle Identity Management binaries that will be upgraded from 11.1.1.2 to 11.1.1.5.

Click **Next**.

4. On the Specify Security Updates screen, enter 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**.

5. The Installation Progress screen shows the progress of the installation. Once the installation is complete, click **Next**.

6. On the Installation Complete Screen, click **Finish** to exit.

4.5 Installing Oracle Fusion Middleware

This section describes how to install Oracle Fusion Middleware.

This section contains the following topics:

- Section 4.5.1, "Installing Oracle Fusion Middleware Components"
- Section 4.5.2, "Installing Oracle Fusion Middleware Home"
- Section 4.5.3, "Installing Oracle WebLogic Server"
- Section 4.5.4, "Installing Oracle Identity Management"

- Section 4.5.5, "Upgrading the Oracle Homes for Oracle Identity Management from 11.1.1.2 to 11.1.1.5"

- Section 4.5.6, "Installing the Oracle SOA Suite"

- Section 4.5.7, "Installing Oracle Identity and Access Management"

> **Note:** Oracle Identity Management products are bundled as two product sets: Oracle Identity Management and Oracle Identity and Access Management.

4.5.1 Installing Oracle Fusion Middleware Components

This section describes how to install the required binaries to create the Middleware home (`MW_HOME`), the Oracle WebLogic Server home (`WL_HOME`), the Oracle homes for Oracle Identity Management Release 11.1.1.5.0 (`IDM_ORACLE_HOME`), the Oracle SOA Suite (`SOA_ORACLE_HOME`) and Oracle Identity and Access Management Release 11.1.1.5.0 (`IAM_ORACLE_HOME`). A summary of these homes is provided in Table 4–3, " Summary of Homes".

Table 4–3   Summary of Homes

Home Name	Home Description	Products Installed
`MW_HOME`	Consists of the Oracle WebLogic Server home and, optionally, one or more Oracle homes.	
`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 with the MW_HOME	■ Oracle WebLogic Server 10.3.5.0
`IDM_ORACLE_ HOME`	Contains the binary and library files for the Oracle Identity Management Release 11.1.1.5.0. Resides within the directory structure of the Middleware Home	■ Oracle Internet Directory ■ Oracle Virtual Directory ■ Oracle DIP ■ ODSM ■ OIF
`IAM_ORACLE_ HOME`	Contains the binary and library files required for Oracle Identity and Access Management Release 11.1.1.5.Resides within the directory structure of the Middleware home	■ OAM ■ OIM ■ OIN
`SOA_ORACLE_ HOME`	Contains the binary and library files required for the Oracle SOA Suite.Required only when creating topologies with OIM.Resides within the directory structure of the Middleware home.	■ SOA
`COMMON_ ORACLE_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

Oracle strongly recommends that you read the release notes for any additional installation and deployment considerations prior to starting the setup process.

4.5.2 Installing Oracle Fusion Middleware Home

As described in Section 2.4, "Shared Storage and Recommended Directory Structure," you install Oracle Fusion Middleware software in at least two storage locations for redundancy.

You must install the following components of Oracle Fusion Middleware to create a Middleware home (`MW_HOME`):

1. Oracle WebLogic Server: Section 4.5.3, "Installing Oracle WebLogic Server"

2. One or more of the Oracle Fusion Middleware components

   a. Section 4.5.4, "Installing Oracle Identity Management"

   b. Section 4.5.7, "Installing Oracle Identity and Access Management"

   c. Section 4.5.6, "Installing the Oracle SOA Suite"

3. Oracle Fusion Middleware for Identity Management

4.5.3 Installing Oracle WebLogic Server

This section describes how to install Oracle WebLogic Server.

4.5.3.1 General Prerequisites for Installing WebLogic

Prior to installing the Oracle WebLogic Server, ensure that your machines meet the system, patch, kernel, and other requirements as specified in *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

4.5.3.2 Prerequisites for Installing the 64-Bit Version

The following prerequisites are required only if you are installing the 64-bit version of Oracle WebLogic Server.

Install Jrockit 64 bit

1. Download Jrockit 64 bit from:

   http://www.oracle.com/technetwork/middleware/jrockit/downloads/index.html

2. Add execute permissions to Jrockit

   ```
   chmod +x jrockit-jdk1.6.0_24-R28.1.3-4.0.1-linux-x64.bin
   ```

3. Start the Jrockit installer by issuing the command:

   ```
   ./jrockit-jdk1.6.0_20-R28.1.0-4.0.1-linux-x64.bin
   ```

4. Click **Next**.

5. Enter the Product Installation Directory. This is inside your Middleware home. For example:

   ```
   /u01/app/oracle/product/fmw/jrockit-jdk1.6.0_20
   ```

6. If you are installing on Windows, you are prompted whether you want to install the JRE for public use. If you want all users to have access to the JRE, select **Yes** otherwise select **No**.

7. Click **Next**.

8. Click **Next** on the Optional Components Screen.

9. Click **Done** when finished.

Additional 64-Bit Prerequisites

1. Download Oracle WebLogic Server Generic from:
   ```
   http://download.oracle.com/otn/nt/middleware/11g/wls/wls1035_
   generic.jar
   ```

2. Add Jrockit to your path for example on Linux issue the command:
   ```
   export PATH=$MW_HOME/jrockit_160_20_R28.1.0-4.0.1/bin;$PATH
   ```

3. Check the version of java by issuing the command:
   ```
   java -version
   ```

   Ensure that the 64 bit version is displayed.

4.5.3.3 Invoking the WebLogic Installer

The first step in the installation procedure is to install Oracle WebLogic Server. The procedure for invoking the Oracle WebLogic installer depends on whether you are installing the 32-bit or 64-bit versions.

Invoking the 32-Bit Installer:

- On UNIX/Linux, issue the command:
  ```
  ./wls_linux32.bin
  ```

- On Windows, execute the command:

```
wls_win32.exe
```

Invoking the 64-Bit Installer

Start the WebLogic installer.

On UNIX or Linux, use the command:

```
java -d64 -jar wls1035_generic.jar
```

On Windows, use the command:

```
java -jar wls1035_generic.jar
```

4.5.3.4 Installing Oracle WebLogic Server

Once you have invoked the installer, proceed as follows.

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

2. On the Choose Middleware Home Screen, select **Create a New Middleware Home**. For the Middleware Home directory enter:

   `MW_HOME/fmw`

   Click **Next**.

> **Note:** `ORACLE_BASE` is the base directory under which Oracle products are installed. The recommended value is `/u01/app/oracle`. See Section 2.4, "Shared Storage and Recommended Directory Structure," for more information.

3. A warning is displayed, indicating that the directory is not empty and asking if you want to proceed. Click **Yes**.

4. On the Register for Security Updates screen, enter your My Oracle Support user name and password so that you can be notified of security updates.

   Click **Next**.

5. On the Choose Install Type screen, select **Typical**.

Note: Oracle WebLogic Server and Oracle Coherence are installed.

   Click **Next**.

6. This step is specific to 64-bit installations. On the JDK selection screen, select the JRockit 64bit JDK that you installed earlier. It should be listed by default.

JDK Selection

JDK(s) chosen will be installed. Defaults will
be used in script string-substitution if installed.

ORACLE

⟳ Dis*c*ard Changes

Bundled JDK:	Approximate installed size*
	Highlighted item:
	All selected bundled JDK's: 0.0 KB
	Total of all selected items: **663.9 MB**
	*Installer requires free disk space approximately 2x this total

Local JDK:

☑ Oracle 1.6.0_20 (/u01/app/.../jrockit-jdk1.6.0_20-R28.1.0-4.0.1)

Browse...

E*x*it   *P*revious   *N*ext

7. On the Choose Product Installation Directories screen, accept the following:

- **Middleware Home Directory**: *ORACLE_BASE*/product/fmw

- **Product Installation Directories for WebLogic Server**: *ORACLE_BASE*/product/fmw/wlserver_10.3

- **Oracle Coherence**: *ORACLE_BASE*/product/fmw/coherence_3.6

Click **Next**.

Choose Product Installation Directories

Provide the directories where you wish to install
WebLogic 10.3.4.0.

ORACLE

⟳ Dis*c*ard Changes

Middleware Home Directory

/u01/app/oracle/product/fmw

Product Installation Directories

The Product Home might contain shared utilities and any products or components for which unique
directories are not set.

WebLogic Server:

/u01/app/oracle/product/fmw/wlserver_10.3   Browse...

Oracle Coherence:

/u01/app/oracle/product/fmw/coherence_3.6   Browse...

E*x*it   *P*revious   *N*ext

8. On the Installation Summary screen, click **Next** to start the install process.

9. On the Installation complete screen, deselect run Quickstart.

   Click **Done** to exit the WebLogic Server Installer

4.5.4 Installing Oracle Identity Management

Perform these steps to install Oracle Identity Management 11.1.1.5 on the hosts identified in Table 4–2, " Software to be Installed for Different Topologies".

Oracle Identity Management consists of:

- Oracle Internet Directory

- Oracle Virtual Directory

- Oracle Directory Integration Platform

- Oracle Directory Services Manager (ODSM)

- Oracle Identity Federation

> **Note:** Because the installation is performed on shared storage, the two MW_HOME installations are accessible and used by the remaining servers in that tier of the topology.
>
> When provisioning the software on the local hard disk of the machine, ensure you complete the steps on all the hosts in the tier.

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

Start the Oracle Fusion Middleware 11*g* Oracle Identity Management Installer as follows:

```
HOST1> runInstaller
```

Then proceed as follows:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:

   - **Specify the Inventory Directory**: /u01/app/oraInventory

   - **Operating System Group Name**: oinstall

   A dialog box appears with the following message:

   ```
   Certain actions need to be performed with root privileges before the
   install can continue. Please execute the script
   /u01/app/oraInventory/createCentralInventory.sh now from another window and
   then press "Ok" to continue the install. If you do not have the root
   privileges and wish to continue the install select the "Continue
   installation with local inventory" option.
   ```

   Log in as root and run:

   ```
   /u01/app/oraInventory/createCentralInventory.sh
   ```

This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

> **Note:** The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, ensure that the following are true:
>
> 1. The /etc/oraInst.loc file exists.
> 2. The Inventory directory listed is valid.
> 3. The user performing the installation has write permissions for the Inventory directory.

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

3. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.

   Click **Next**.

4. On the Select Installation Type screen, select **Install Software - Do Not Configure**, and then click **Next**.

5. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.

6. On the Specify Installation Location screen, enter the following values:

   - **Oracle Middleware Home**: Select the previously installed Middleware home from the list for MW_HOME, for example:

     /u01/app/oracle/product/fmw

   - **Oracle Home Directory**: Enter idm as the Oracle home directory name.

   Click **Next**.

7. On the Installation Summary screen, click **Install**.

8. On the Installation Progress screen, on Linux and UNIX systems, a dialog box appears that prompts you to run the oracleRoot.sh script. Open a window and run the oracleRoot.sh script, as the root user.

9. On the Installation Complete screen, click **Finish**.

4.5.5 Upgrading the Oracle Homes for Oracle Identity Management from 11.1.1.2 to 11.1.1.5

The Oracle home for Oracle Identity Management 11.1.1.2 (IDM_ORACLE_HOME) must be upgraded to Release 11.1.1.5 before creating the Identity Management domain. This section provides the steps to upgrade the IDM_ORACLE_HOME.

Follow the steps in this section to upgrade the IDM_ORACLE_HOME from Release 11.1.1.2 to 11.1.1.5 using Oracle Universal Installer. Complete these step on IDMHOST1 and IDMHOST2. Ensure that your machines meet all the prerequisites listed in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*. Start the Oracle Identity Management Patch Set installer as follows:

```
HOST1> ./runInstaller
```

Then proceed as follows

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

2. On the Specify Installation Location screen, enter the following values:

   ■ **Oracle Middleware Home**: Select the previously installed Middleware Home from the list, for example: `/u01/app/oracle/product/fmw`

   ■ **Oracle Home Directory**: Enter `IDM` as the Oracle home directory. This Oracle home contains the Oracle Identity Management binaries that will be upgraded from 11.1.1.2 to 11.1.1.5.

   Click **Next**.

3. On the Specify Security Updates screen, enter 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**.

4. On the Installation Summary screen, click **Install**.

5. On Installation Progress Screen click **Next**.

   On Linux and UNIX systems, you are prompted to execute `oracleRoot.sh` as the `root` user. During the running of this script, you will be asked:

   ```
   Do you want to run oidRoot.sh to configure OID for privileged ports? (yes/no)
   ```

   Reply `yes`, as the Oracle Internet Directory port is `389`, which is a privileged port. Execute `oracleRoot.sh` as the `root` user.

6. On the Installation Complete screen, click **Finish**.

4.5.6 Installing the Oracle SOA Suite

Perform these steps to install the Oracle SOA Suite on `IDMHOST1`, `IDMHOST2`, `OIMHOST1`, and `OIMHOST2`.

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

On UNIX and Linux systems, start the Oracle Fusion Middleware 11*g* SOA Suite Installer as follows:

```
HOST1>./runInstaller
```

On Windows, the command is:

```
setup.exe
```

When the installer prompts you for a JRE/JDK location, enter the Oracle SDK location created in the Oracle WebLogic Server installation, for example:

```
/u01/app/oracle/product/fmw/jrockit_version
```

Then perform these installation steps:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:

   ■ **Specify the Inventory Directory**: `/u01/app/oraInventory`

- **Operating System Group Name**: `oinstall`

A dialog box appears with the following message:

```
Certain actions need to be performed with root privileges before the install
can continue. Please execute the script
/u01/app/oraInventory/createCentralInventory.sh now from another window and
then press "Ok" to continue the install. If you do not have the root privileges
and wish to continue the install select the "Continue installation with local
inventory" option.
```

Log in as `root` and run:

```
/u01/app/oraInventory/createCentralInventory.sh
```

This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

Note: The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, check the following:

1. The `/etc/oraInst.loc` file exists.
2. The Inventory directory listed is valid.
3. The user performing the installation has write permissions for the Inventory directory.

---

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

3. On the Install Software Updates screen, choose whether to register with Oracle Support for updates or to search for updates locally.

4. On the Prerequisite Checks screen, verify that the checks complete successfully, and then click **Next**.

5. On the Specify Installation Location screen, enter the following values:

   - **Oracle Middleware Home**: Select a previously installed Middleware Home from the drop-down list. For example: `/u01/app/oracle/product/fmw`

   - **Oracle Home Directory**: Enter `SOA` as the Oracle home directory name.

   - Click **Next**.

6. On the Application Server screen, choose your Application Server, for example: Web Logic Server.

   Click **Next**.

7. On the Installation Summary screen, click **Install**.

8. On the Installation Process screen, click **Next**.

9. On the Installation Complete screen, click **Finish**.

4.5.7 Installing Oracle Identity and Access Management

Oracle Identity and Access Management consists of the following products:

- Oracle Access Manager 11*g*
- Oracle Identity Manager

Perform the steps in this section to install Oracle Identity and Access Management on the hosts identified in Table 4–1, " Software Versions Used".

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

Start the Oracle Fusion Middleware 11*g* Installer for Oracle Identity and Access Management as follows:

```
HOST1>./ runInstaller
```

When the installer prompts you for a JRE/JDK location, enter the Oracle SDK location created in the Oracle WebLogic Server installation, for example:

```
/u01/app/oracle/product/fmw/jrockit_version
```

Then perform these installation steps:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:

   - **Specify the Inventory Directory**: `/u01/app/oraInventory`

   - **Operating System Group Name**: `oinstall`

   A dialog box appears with the following message:

   ```
   Certain actions need to be performed with root privileges before the install
   can continue. Please execute the script
   /u01/app/oraInventory/createCentralInventory.sh now from another window and
   then press "Ok" to continue the install. If you do not have the root privileges
   and wish to continue the install select the "Continue installation with local
   inventory" option.
   ```

   Log in as `root` and run:

   ```
   /u01/app/oraInventory/createCentralInventory.sh
   ```

   This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

   > **Note:** The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, check the following:
   >
   > 1. The `/etc/oraInst.loc` file exists.
   >
   > 2. The Inventory directory listed is valid.
   >
   > 3. The user performing the installation has write permissions for the Inventory directory.

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

3. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.

   Click **Next**.

4. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.

5. On the Specify Installation Location screen, enter the following values:

   - **Oracle Middle Ware Home**: Select a previously installed Middleware Home from the drop-down list. For example: `/u01/app/oracle/product/fmw`

   - **Oracle Home Directory**: Enter `iam` as the Oracle home directory name.

   Click **Next**.

6. On the Installation Summary screen, click **Install**.

7. On the Installation Progress screen, click **Next**.

8. On the Installation Complete screen, click **Finish**.

4.6 Patching the Software

This section describes how to apply patches after installing the software. For a complete list of patches, see the Oracle Fusion Middleware Release Notes for your platform and operating system.

This section contains the following topics:

- Section 4.6.1, "Provisioning the OIM Login Modules Under the WebLogic Server Library Directory"

- Section 4.6.2, "Creating the wlfullclient.jar File"

4.6.1 Provisioning the OIM Login Modules Under the WebLogic Server Library Directory

Due to issues with versions of the configuration wizard, some environmental variables are not added to the *DOMAIN_HOME*/bin/setDomainenv.sh script. This causes certain install sequences to fail. This section is a temporary workaround for that problem. The steps in this section must be performed on all the hosts in application tier (IDMHOST1, IDMHOST2, OIMHOST1, OIMHOST2, OIFHOST1, and OIFHOST2).

Apply the following steps across all the WebLogic Server homes in the domain.

1. Copy the `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsigmbean.jar` and `oimsignaturembean.jar` files located under the *IAM_ORACLE_HOME*/server/loginmodule/wls directory to the *MW_HOME*/wlserver_10.3/server/lib/mbeantypes directory.

   ```
   cp $IAM_ORACLE_HOME/server/loginmodule/wls/* $MW_HOME/wlserver_
   10.3/server/lib/mbeantypes/.
   ```

2. Change directory to *MW_HOME*/wlserver_10.3/server/lib/mbeantypes/.

   ```
   cd $MW_HOME/wlserver_10.3/server/lib/mbeantypes
   ```

3. Change the permissions on these files to 750 by using the `chmod` command.

   ```
   chmod 750 *
   ```

4.6.2 Creating the wlfullclient.jar File

Oracle Identity Manager uses the `wlfullclient.jar` library for certain operations. Oracle does not ship this library, so you must create this library manually. Oracle recommends creating this library under the *MW_HOME*/wlserver_10.3/server/lib directory on all the machines in the application tier of your

environment. You do not need to create this library on directory tier machines such as `OIDHOST1`, `OIDHOST2`, `OVDHOST1` and `OVDHOST2`.

Follow these steps to create the `wlfullclient.jar` file:

1. Navigate to the *MW_HOME*`/wlserver_10.3/server/lib` directory

2. Set your `JAVA_HOME` environment variable t and ensure that the `JAVA_HOME/bin` directory is in your path.

3. Create the `wlfullclient.jar` file by running:

    ```
    java -jar wljarbuilder.jar
    ```

4.7 Backing Up the Installation

It is a best practice recommendation to back up the Middleware Home and the Oracle Homes. On Linux, to create a backup of the `MW_HOME` and the `ORACLE_HOME`s, as the `root` user, type:

```
tar -cvpf fmwhomeback.tar ORACLE_BASE/product/fmw
```

This creates a backup of the installation files for any products installed in the Oracle Fusion Middleware home.

5

Configuring the Web Tier

This chapter describes how to configure the Oracle Web Tier.

Follow these steps to configure the Oracle HTTP Server on Webhost1 and Webhost2.

This chapter includes the following topics:

- Section 5.1, "Configuring the Oracle Web Tier"
- Section 5.2, "Configuring Virtual Hosts"
- Section 5.3, "Configuring Oracle HTTP Server to Run as Software Owner"
- Section 5.4, "Validating the Installation"
- Section 5.5, "Backing up the Web Tier Configuration"

5.1 Configuring the Oracle Web Tier

The steps for configuring the Oracle Web Tier are the same for `WEBHOST1` and `WEBHOST2`.

This section contains the following topics:

- Section 5.1.1, "Configuring the HTTP Server"
- Section 5.1.2, "Validating the Installation"

5.1.1 Configuring the HTTP Server

Perform these steps to configure the Oracle web tier:

1. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

   ```
   WEBHOST1> cd WEB_ORACLE_HOME/bin
   ```

2. Start the Configuration Wizard:

   ```
   WEBHOST1> ./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 **NOT** selected.

   Ensure Oracle Web Cache is **NOT** selected.

Click **Next**.

3. On the Specify Component Details screen, specify the following values:

    Enter the following values for `WEBHOST1`:

    - `Instance Home Location:` `/u01/app/oracle/admin/ohs_inst1`
    - `Instance Name:` `ohs_inst1`
    - `OHS Component Name:` `ohs1`

    Enter the following values for `WEBHOST2`:

    - Instance Home Location: `/u01/app/oracle/admin/ohs_inst2`
    - Instance Name: `ohs_inst2`
    - OHS Component Name: `ohs2`

    Click **Next**.

4. On the Configure Ports screen, use a file to specify the ports to be used so that you can bypass automatic port configuration. You do this to have all of the ports used by the various components synchronized across hosts, which is advisable but not mandatory in High Availability implementations, Select a file name and then click **View/Edit**. Enter the following text into the file:

    ```
    [OHS]
    #Listen port for OHS component
    OHS Port = 7777
    [OPMN]
    #OPMN Local port no
    OPMN Local Port = 6700
    ```

    You can find a sample `staticports.ini` file on installation Disk1 in the `stage/Response` directory.

    Click **Save**, then click **Next**.

5. 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**.

6. 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.

5.1.2 Validating the Installation

After the installation is completed, check that you can access the Oracle HTTP Server home page using the following URLs:

`http://webhost1.mycompany.com:7777/`

```
http://webhost2.mycompany.com:7777/
```

5.2 Configuring Virtual Hosts

In order for Oracle Identity Management to work with the load balancer, you must create two virtual hosts.

To do so, create a file called `virtual_hosts.conf` in *ORACLE_INSTANCE*`/config/OHS/`*component*`/moduleconf`.

On `WEBHOST1` and `WEBHOST2`, add the following entries to the file:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName https://sso.mycompany.com:443
   RewriteEngine On
   RewriteOptions inherit
   UseCanonicalName On
</VirtualHost>

<VirtualHost *:7777>
   ServerName http://oiminternal.mycompany.com:80
   RewriteEngine On
   RewriteOptions inherit
   UseCanonicalName On
</VirtualHost>
```

5.3 Configuring Oracle HTTP Server to Run as Software Owner

By default, the Oracle HTTP server runs as the user `nobody`. In the Identity Management installation, the Oracle HTTP server should run as the Software owner and group.

To cause it to run as the appropriate user and group, edit the file `httpd.conf`, which is located in *ORACLE_INSTANCE*`/config/OHS/`*component_name*.

Find the section in `http.conf` where `User` is defined.

Change this section to read:

```
User User_who_installed_the_software
Group Group_under_which_the_HTTP_server_runs
```

`Group` is typically the default user group, for example: `oinstall`.

For example:

```
<IfModule !mpm_winnt_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# . On SCO (ODT 3) use "User nouser" and "Group nogroup".
# . On HPUX you may not be able to use shared memory as nobody, and the
# suggested workaround is to create a user www and use that user.
# NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
# when the value of (unsigned)Group is above 60000;
# don't use Group #-1 on these systems!
#
User oracle
Group oinstall
```

```
</IfModule>
```

Restart the Oracle HTTP Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

5.4 Validating the Installation

Once the installation is completed check that the it is possible to access the Oracle HTTP Server through the following URL's.

```
http://webhost1.mycompany.com:7777/
```

```
http://webhost2.mycompany.com:7777/
```

```
https://sso.mycompany.com/
```

```
http://oiminternal.mycompany.com
```

5.5 Backing up the Web 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*.

To back up the web tier installation, follow these steps,

1. Shut down the instance as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. Back up the Middleware home on the web tier. On Linux, use the following command, as `root`:

   ```
   tar -cvpf BACKUP_LOCATION/web.tar MW_HOME
   ```

3. Back up the Instance home on the web tier using the following command, as `root`:

   ```
   tar -cvpf BACKUP_LOCATION/web_instance.tar ORACLE_INSTANCE
   ```

4. Start the instance as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

   > **Note:** Create backups on all machines in the web tier by following the steps shown.

For information about backing up the application tier configuration, see Section 19.4, "Performing Backups and Recoveries."

6

Creating the WebLogic Server Domain for Identity Management

This chapter describes how to create a domain using the Configuration Wizard, Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. You can extend the domain to add Oracle Fusion Middleware components such as Oracle Identity Manager and Oracle Access Manager.

> **Note:** Oracle strongly recommends that you read the release notes for any additional installation and deployment considerations prior to starting the setup process.

This chapter contains the following sections.

6.1 Enabling ADMINVHN on IDMHOST1

Note that this step is 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, `ADMINVHN.mycompany.com`. Check that `ADMINVHN.mycompany.com` is enabled on `IDMHOST1`.

Linux

To enable the virtual IP address, run the following commands as `root`:

```
/sbin/ifconfig interface:index IPAddress netmask netmask
/sbin/arping -q -U -c 3 -I interface IPAddress
```

where *interface* is `eth0`, `eth1`, and so forth, and *index* is `0`, `1`, `2`, and so forth.

For example:

```
/sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
```

Enable your network to register the new location of the virtual IP address:

```
/sbin/arping -q -U -c 3 -I eth0 100.200.140.206
```

Validate that the address is available by `pinging` it from another node, for example:

```
/bin/ping 100.200.140.206
```

Windows

To enable the virtual IP address, run the following command:

```
netsh interface ip add address interface IP_Address netmask
```

where `IP_Address` is the virtual IP address and the `netmask` is the associated netmask.

In the following example, the IP address is enabled on the interface `Local Area Connection`.

```
netsh interface ip add address "Local Area connection" 100.200.140.206
255.255.255.0
```

6.2 Running the Configuration Wizard on IDMHOST1 to Create a Domain

Run the Configuration Wizard from the Oracle Common home directory to create a domain containing the Administration Server. Later, you will extend the domain to contain other components.

1. Change directory to the location of the Configuration Wizard. This is within the Oracle Common Home directory (created in Chapter 4, "Installing the Software").

   ```
   IDMHOST1> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
   ```

2. Start the Oracle Fusion Middleware Configuration Wizard

   On Linux, type:

   ```
   IDMHOST1> ./config.sh
   ```

On Windows, type:

```
IDMHOST1> ./config.cmd
```

3. On the Welcome screen, select **Create a New WebLogic Domain**, and click **Next**.

4. The Select Domain Source screen is displayed in Figure 6–1.

Figure 6–1   Select Domain Source Screen
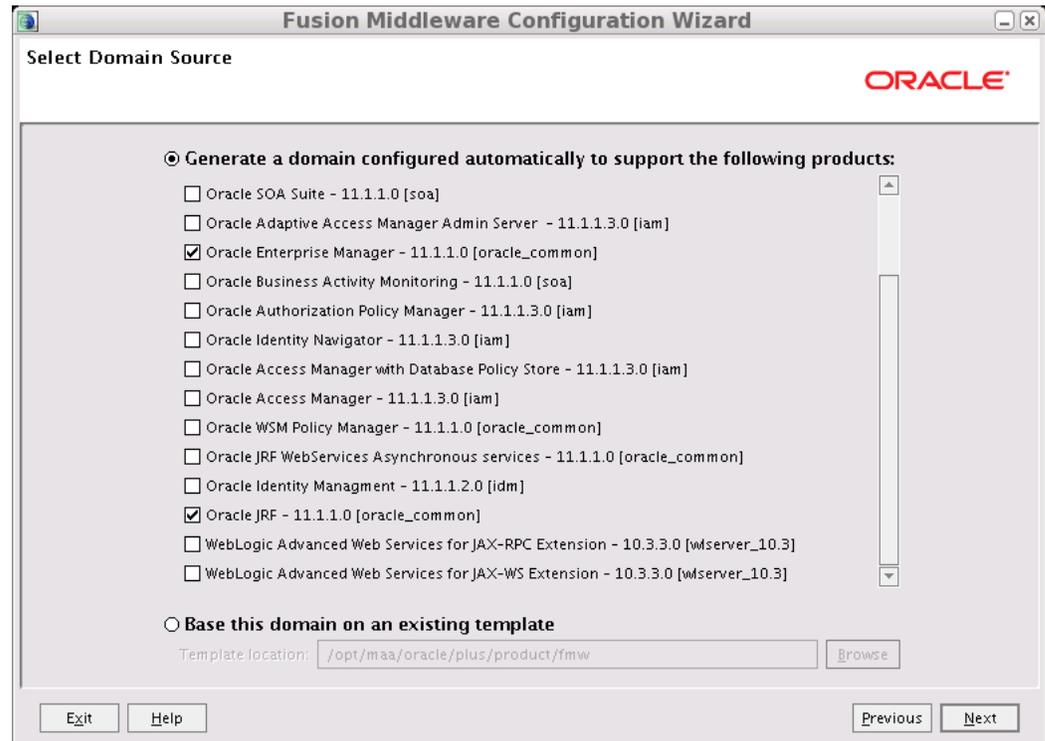
On the Select Domain Source screen, do the following:

- Select **Generate a domain configured automatically to support the following products**.

- Select the following products:

    - **Basic WebLogic Server Domain [wlserver_10.3]** (This should be selected automatically.)

    - **Oracle Enterprise Manager [oracle_common]**

    - **Oracle JRF [oracle_common]** (This should be selected automatically.)

Click **Next**.

5. On the Specify Domain Name and Location screen, enter the domain name (*IDMDomain*).

Ensure that the domain directory matches the directory and shared storage mount point recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

Enter

```
ORACLE_BASE/admin/IDMDomain/aserver/
```

for the domain directory and

ORACLE_BASE/admin/*IDMDomain*/aserver/applications

for the application directory. This directory should be in shared storage.

6. Click **Next**.

7. On the Configure Administrator Username and Password screen, enter the username (default is `weblogic`) and password to be used for the domain's administrator. For example:

   - **Name**: `weblogic`

   - **User Password**: *password for weblogic user*

   - **Confirm User Password**: *password for weblogic user*

   - **Description**:`This user is the default administrator.`

   Click **Next**.

8. On the Configure Server Start Mode and JDK screen, do the following:

   - For WebLogic Domain Startup Mode, select **Production Mode**.

   - For JDK Selection, select **Jrockit SDK**

   Click **Next**.

9. On the Select Optional Configuration screen, select the following:

   - **Administration Server**

   - **Managed Servers, Clusters and Machines**

   Click **Next**.

10. On the Configure the Administration Server screen, enter the following values:

    - **Name**: **AdminServer**

    - **Listen Address**: **ADMINVHN.mycompany.com**.

    - **Listen Port**: **7001**

    - **SSL listen port**: **N/A**

    - **SSL enabled**: unchecked

    Click **Next**.

11. On the Configure Managed Servers screen, click **Next**

12. On the Configure Clusters screen, click **Next**

13. On the Configure Machines screen, click the **Unix Machine** tab (for Linux and UNIX machines) or the **Machines** tab (for Windows machines) and then click **Add** to add the following machine. The machine name does not need to be a valid host name or listen address, it is just a unique identifier of a node manager location:

    - **Name**: `ADMINHOST`.

    - **Node manager listen address**: `localhost`

    Leave all other fields to their default values.

14. Click **Next**.

15. On the Assign Servers to Machines screen, assign servers to machines as follows:

- **ADMINHOST**: **AdminServer**

Click **Next**.

16. On the Configuration Summary screen, validate that your choices are correct, then click **Create**.

17. On the Create Domain screen, click **Done**.

6.3 Creating boot.properties for the WebLogic Administration Server on IDMHOST1

Create a `boot.properties` file for the Administration Server on `IDMHOST1`. The `boot.properties` file enables the Administration Server to start without prompting you for the administrator username and password.

For the Administration Server:

1. Create the following directory structure.

   ```
   mkdir -p ORACLE_
   BASE/admin/IDMDomain/aserver/IDMDomain/servers/AdminServer/security
   ```

2. In a text editor, create a file called boot.properties in the last directory created in the previous step, and enter the username and password in the file. For example:

   ```
   username=weblogic
   password=password for weblogic user
   ```

   > **Note:** The username and password entries in the file are not encrypted until you start the Administration Server, as described in Section 6.5, "Updating the Node Manager Credentials." For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, start the server as soon as possible so that the entries are encrypted.

6.4 Starting Node Manager on IDMHOST1

Perform these steps to start Node Manager on `IDMHOST1`:

1. Run the `startNodeManager.sh` script located under the `ORACLE_BASE/product/fmw/wlserver_10.3/server/bin/` directory.

2. Run the `setNMProps.sh` script on `IDMHOST1` to set the `StartScriptEnabled` property to `true`:

   ```
   cd MW_HOME/oracle_common/common/bin
   ./setNMProps.sh
   ```

   > **Note:** You must use the `StartScriptEnabled` property to avoid class loading failures and other problems.

3. Stop the Node Manager by killing the Node Manager process, or stop the service in Windows.

4. Start Node Manager for the Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

6.5 Updating the Node Manager Credentials

You start the Administration server by using `wlst` and connecting to Node Manager. The first start of the Administration Server with Node Manager, however, requires that you change the default username and password that the Configuration Wizard sets for Node Manager. Therefore you must use the start script for the Administration Server for the first start. Follow these steps to start the Administration Server using Node Manager.

Steps 1-4 are required for the first start operation, but subsequent starts require only Step 4.

1. Start the Administration Server using the start script in the domain directory.

```
IDMHOST1> cd ORACLE_BASE/admin/domain_name/aserver/domain_name/bin
IDMHOST1> ./startWebLogic.sh
```

2. Use the Administration Console to update the Node Manager credentials.

   a. In a browser, go to `http://ADMINVHN.mycompany.com:7001/console`.

   b. Log in as the administrator.

   c. Click **Lock and Edit**.

   d. Click **Domain_name**->**Security**->**General** and expand **Advanced** at the bottom.

   e. Enter a new username for Node Manager or make a note of the existing one and update the Node Manager password.

   f. Save and activate the changes.

3. Stop the WebLogic Administration Server by issuing the command `stopWebLogic.sh` located under the `ORACLE_BASE`/admin/domain_name/aserver/domain_name/bin directory.

4. Start WLST and connect to the Node Manager with `nmconnect` and the credentials you just updated. Then start the WebLogic Administration Server using `nmstart`.

```
IDMHOST1> cd ORACLE_COMMON_HOME/common/bin
IDMHOST1> ./wlst.sh
```

On Windows, the command is:

```
wlst.cmd
```

Once in the `wlst` shell, execute the following commands:

```
wls:/offline> nmConnect('Admin_User','Admin_Pasword', 'IDMHOST1','5556',
  'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
wls:/nm/domain_name> nmStart('AdminServer')
```

where `Admin_user` and `Admin_Password` are the Node Manager username and password you entered in Step 2.

> **Note:** `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 *ORACLE_BASE*`/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties` file.

6.6 Validating the WebLogic Administration Server

Perform these steps to ensure that the Administration Server is properly configured:

1. In a browser, go to `http://ADMINVHN.mycompany.com:7001/console`.

2. Log in as the WebLogic administrator, for example: `weblogic`.

3. Check that you can access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.

4. Log in to Oracle Enterprise Manager Fusion Middleware Control as the WebLogic administrator, for example: `weblogic`.

6.7 Disabling Host Name Verification for the Oracle WebLogic Administration Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. (See Chapter 15, "Setting Up Node Manager.") If you have not configured the server certificates, you will receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the EDG topology configuration is complete as described in Chapter 15, "Setting Up Node Manager."

Perform these steps to disable host name verification:

1. Go to the Oracle WebLogic Server Administration Console at:

   `http://adminvhn.us.oracle.com:7001/console`

2. Log in as the user `weblogic`, using the password you specified during the installation.

3. Click **Lock** and **Edit**.

4. Expand the Environment node in the Domain Structure window.

5. Click **Servers**. The Summary of Servers page appears.

6. Select **AdminServer(admin)** in the **Name** column of the table. The Settings page for AdminServer(admin) appears.

7. Click the **SSL** tab.

8. Click **Advanced**.

9. Set Hostname Verification to **None**.

10. Click **Save**.

11. Click **Activate Changes**.

6.8 Stopping and Starting the WebLogic Administration Server

1. Stop the Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components"

2. Start WLST and connect to the Node Manager with nmconnect and the credentials set previously described. Then start the Administration Server using `nmstart`.

    ```
    IDMHOST1> cd ORACLE_COMMON_HOME/common/bin
    IDMHOST1> ./wlst.sh
    ```

    Once in the `wlst` shell, execute the following commands:

    ```
    wls:/offline> nmConnect('Admin_User','Admin_Pasword', 'IDMHOST1','5556',
      'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
    wls:/nm/domain_name> nmStart('AdminServer')
    ```

    where `Admin_user` and `Admin_Password` are the Node Manager username and password you entered in Step 2 of Section 6.5, "Updating the Node Manager Credentials."

    > **Note:** `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 `ORACLE_BASE`/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties file.

6.9 Configuring Oracle HTTP Server for the WebLogic Administration Server

To enable Oracle HTTP Server to route to the Administration Server, you must set the the corresponding mount points in your HTTP Server configuration.

1. On each of the web servers on `WEBHOST1` and `WEBHOST2` create a file called admin.conf in the directory:

    ```
    ORACLE_INSTANCE/config/OHS/component/moduleconf
    ```

    This file has the following entries:

    ```
    NameVirtualHost *:7777

    <VirtualHost *:7777>

        ServerName admin.mycompany.com:80
        ServerAdmin you@your.address
        RewriteEngine On
        RewriteOptions inherit
        RewriteRule ^/console/jsp/common/logout.jsp /oamsso/logout.html [PT]
        RewriteRule ^/em/targetauth/emaslogout.jsp /oamsso/logout.html [PT]

    # Admin Server and EM
        <Location /console>
           SetHandler weblogic-handler
           WebLogicHost ADMINVHN.mycompany.com
           WeblogicPort 7001
        </Location>
    ```

```
                        <Location /consolehelp>
                           SetHandler weblogic-handler
                           WebLogicHost ADMINVHN.mycompany.com
                           WeblogicPort 7001
                        </Location>

                        <Location /em>
                           SetHandler weblogic-handler
                           WebLogicHost ADMINVHN.mycompany.com
                           WeblogicPort 7001
                        </Location>

                     </VirtualHost>
```

Notes:

- Values such as `admin.mycompany:80` and `you@youraddress` that are noted in this document serve as examples only. Enter values based on the actual environment.

- If you are not using a virtual host for your Administration Server host (single instance), replace `ADMINVHN.mycompany.com` with `IDMHOST1.mycompany.com`.

- The `RewriteRule` entries are only necessary if your topology includes Oracle Access Manager.

---

2. Restart Oracle HTTP Server on both `WEBHOST1` and `WEBHOST2`, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

    ```
    WEBHOST1> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
    ias-component=ohs1

    WEBHOST2> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
    ias-component=ohs2
    ```

6.10 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the Oracle HTTP server, you must register the Oracle HTTP server with the domain. To do this, you must register Oracle HTTP Server with WebLogic Server using the following command:

```
WEBHOST1> cd ORACLE_BASE/admin/instance_name/bin
WEBHOST1> ./opmnctl registerinstance -adminHost ADMINVHN.mycompany.com \
   -adminPort 7001 -adminUsername weblogic
```

You must also run this command from `WEBHOST2` for `OHS2`.

6.11 Setting the Front End URL for the Administration Console

Oracle WebLogic Server Administration Console tracks changes that are made to ports, channels and security using the console. When changes made through the console are activated, the console validates its current listen address, port and protocol. If the listen address, port and protocol are still valid, the console redirects the HTTP request, replacing the host and port information with the Administration Server's listen address and port. When the Administration Console is accessed using a

load balancer, you must change the Administration Server's front end URL so that the user's browser is redirected to the appropriate load balancer address. To make this change, perform the following steps:

1. Log in to Oracle WebLogic Server Administration Console.

2. Click **Lock and Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers** to open the Summary of Servers page.

5. Select **Admin Server** in the Names column of the table. The Settings page for AdminServer(admin) appears.

6. Click the **Protocols** tab.

7. Click the **HTTP** tab.

8. Set the **Front End Host** field to `admin.mycompany.com` (your load balancer address).

9. Set **FrontEnd HTTP Port** to `80`

10. Save and activate the changes.

To eliminate redirections, best practice is to disable the Administration console's `Follow changes` feature. To do this, log in to the administration console and click **Preferences**->**Shared Preferences**. Deselect **Follow Configuration Changes** and click **Save**.

6.12 Enabling WebLogic Plug-in

In Enterprise deployments, Oracle WebLogic Server is fronted by Oracle HTTP servers. The HTTP servers are, in turn, fronted by a load balancer, which performs SSL translation. In order for internal loopback URLs to be generated with the `https` prefix, Oracle WebLogic Server must be informed that it receives requests through the Oracle HTTP Server WebLogic plug-in.

The plug-in can be set at either the domain, cluster, or Managed Server level. Because all requests to Oracle WebLogic Server are through the Oracle OHS plug-in, set it at the domain level.

To do this perform the following steps:

1. Log in to the Oracle WebLogic Server Administration Console at:

    `http://ADMINVHN.mycompany.com:7001/console`

2. Click **Lock and Edit**.

3. Click **IDMDomain** In the Domain Structure Menu.

4. Click the **Configuration** tab.

5. Click the **Web Applications** sub tab.

6. Select **WebLogic Plug-in Enabled**.

7. Click **Save** and **Activate the Changes**.

8. Restart WebLogic Administration Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

6.13 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as `Running` in the Administration Console. If the server is shown as `Starting` or `Resuming`, wait for the server status to change to `Started`. If another status is reported (such as `Admin` or `Failed`), check the server output log files for errors. See Section 19.6, "Troubleshooting" for possible causes.

Validate Administration Console and Oracle Enterprise Manager Fusion Middleware Control through Oracle HTTP Server using the following URLs:

- http://admin.mycompany.com/console

- http://admin.mycompany.com/em

For information on configuring system access through the load balancer, see Section 2.2.1, "Load Balancers."

> **Note:**   After registering the Oracle HTTP Server as described in Section 6.10, "Registering Oracle HTTP Server with WebLogic Server," the Oracle HTTP Server should appear as a manageable target in Oracle Enterprise Manager Fusion Middleware Control. To verify this, log in to Fusion Middleware Control. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

6.14 Manually Failing Over the WebLogic Administration Server

This section discusses how to fail over the Administration Server to `IDMHOST2` and how to fail it back to `IDMHOST1`.

This section contains the following topics:

- Section 6.14.1, "Failing over the Administration Server to IDMHOST2"

- Section 6.14.2, "Starting the Administration Server on IDMHOST2"

- Section 6.14.3, "Validating Access to IDMHOST2 Through Oracle HTTP Server"

- Section 6.14.4, "Failing the Administration Server Back to IDMHOST1"

6.14.1 Failing over the Administration Server to IDMHOST2

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 `IDMHOST1` to `IDMHOST2`.

Assumptions:

- The Administration Server is configured to listen on `ADMINVHN.mycompany.com`, and not on `ANY` address. See step 10 in Section 6.2, "Running the Configuration Wizard on IDMHOST1 to Create a Domain."

- The Administration Server is failed over from `IDMHOST1` to `IDMHOST2`, and the two nodes have these IP addresses:

  - `IDMHOST1`: `100.200.140.165`

  - `IDMHOST2`: `100.200.140.205`

  - `ADMINVIP`: `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 `IDMHOST1` and `IDMHOST2`.

■ The domain directory where the Administration Server is running in `IDMHOST1` is on a shared storage and is mounted also from `IDMHOST2`.

> **Note:** NM in `IDMHOST2` does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on `IDMHOST2`. 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 `IDMHOST2` as described in previous chapters. That is, the same path for `ORACLE_HOME` and `MW_HOME` that exists in `IDMHOST1` is available in `IDMHOST2`.

The following procedure shows how to fail over the Administration Server to a different node, `IDMHOST2`.

Linux

1. Stop the Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. Migrate the IP address to the second node.

   a. Run the following command as root on `IDMHOST1` (where *x*:*y* is the current interface used by `ADMINVHN.mycompany.com`):

   ```
   IDMHOST1 > /sbin/ifconfig x:y down
   ```

   For example:

   ```
   IDMHOST1 > /sbin/ifconfig eth0:1 down
   ```

   b. Run the following command on `IDMHOST2`:

   ```
   IDMHOST2> /sbin/ifconfig interface:index IP_Address netmask netmask
   ```

   For example:

   ```
   /sbin/ifconfig eth0:1 10.0.0.1 netmask 255.255.255.0
   ```

   > **Note:** Ensure that the netmask and interface to be used match the available network configuration in `IDMHOST2`.

3. Update routing tables by using `arping`, for example:

   ```
   IDMHOST2> /sbin/arping -b -A -c 3 -I eth0 10.0.0.1
   ```

Windows

1. Stop the Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. Migrate the IP address to the second node.

   a. Run the following command as root on `IDMHOST1`

```
netsh interface ip delete address interface netmask
```

In the following example, the IP address is disabled on the interface Local Area Connection:

```
netsh interface ip delete address "Local Area connection" 100.200.140.206
```

b. Run the following command on IDMHOST2:

```
netsh interface ip add address interface IP_Address netmask
```

In the following example, the IP address is enabled on the interface Local Area Connection:

```
netsh interface ip add address "Local Area connection" 100.200.140.206
255.255.255.0
```

6.14.2 Starting the Administration Server on IDMHOST2

Perform the following steps to start Node Manager on IDMHOST2:

1. On IDMHOST1, unmount the Administration Server domain directory. For example:

```
umount /u01/app/oracle/admin/IDMDomain/aserver/
```

2. On IDMHOST2, mount the Administration Server domain directory. For example:

```
mount /u01/app/oracle/admin/IDMDomain/aserver/
```

3. Start Node Manager by using the following commands:

```
IDMHOST2> cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
IDMHOST2> ./startNodeManager.sh
```

4. Stop Node Manager.

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.

---

5. Run the setNMProps.sh script to set the StartScriptEnabled property to true before starting Node Manager:

```
cd MW_HOME/oracle_common/common/bin
./setNMProps.sh
```

Note: You must use the StartScriptEnabled property to avoid class loading failures and other problems.

---

6. Start the Node Manager as described in Section 19.1.5.3, "Starting Node Manager for an Administration Server."

7. Start the Administration Server on IDMHOST2.

```
DMHOST2> cd ORACLE_COMMON_HOME/common/bin
```

```
IDMHOST2> ./wlst.sh
```

Once in the `wlst` shell, execute the following commands:

```
wls:/offline> nmConnect(Admin_User,'Admin_Password, IDMHOST2,'5556',
'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
wls:/nm/domain_name> nmStart('AdminServer')
```

8. Test that you can access the Administration Server on IDMHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.

   b. Check that you can access and verify the status of components in the Oracle Enterprise Manager at `http://ADMINVHN.mycompany.com:7001/em`.

6.14.3 Validating Access to IDMHOST2 Through Oracle HTTP Server

Perform the same steps as in Section 6.13, "Validating Access Through Oracle HTTP Server." This is to check that you can access the Administration Server when it is running on IDMHOST2.

6.14.4 Failing the Administration Server Back to IDMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on IDMHOST2 and run it on IDMHOST1. To do this, migrate ADMINVHN back to IDMHOST1 node as follows:

1. On IDMHOST2, unmount the Administration server domain directory. For example:

   ```
   umount /u01/app/oracle/admin/IDMDomain/aserver/
   ```

2. On IDMHOST1, mount the Administration server domain directory. For example:

   ```
   mount /u01/app/oracle/admin/IDMDomain/aserver/
   ```

3. Ensure that the Administration Server is not running. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from *DOMAIN_HOME*/bin.

4. Stop the Administration server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

5. Disable the ADMINVHN.mycompany.com virtual IP address on IDMHOST2 and run the following command as `root` on IDMHOST2:

   ```
   IDMHOST2 > /sbin/ifconfig x:y down
   ```

   where `x:y` is the current interface used by ADMINVHN.mycompany.com.

6. Run the following command on IDMHOST1:

   ```
   IDMHOST1> /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 IDMHOST1

7. Update routing tables by using arping. Run the following command from IDMHOST1.

```
IDMHOST1> /sbin/arping -b -A -c 3 -I interface 100.200.140.206
```

8. If Node Manager is not already started on `IDMHOST1`, start it, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

9. Start the Administration Server again on `IDMHOST1`.

```
IDMHOST1> cd ORACLE_COMMON_HOME/common/bin
IDMHOST1> ./wlst.sh
```

Once in the `wlst` shell, execute

```
wls:/offline>nmConnect(Admin_User,'Admin_Pasword, IDMHOST1,'5556',
      'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain'
wls:/nm/domain_name> nmStart('AdminServer')
```

10. Test that you can access the Oracle WebLogic Server Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.

11. Check that you can access and verify the status of components in the Oracle Enterprise Manager at `http://ADMINVHN.mycompany.com:7001/em`.

6.15 Backing Up the WebLogic Domain

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 about database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation at this point, complete these steps:

1. Back up the web tier as described in Section 5.5, "Backing up the Web Tier Configuration."

2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.

3. Stop Node Manager and all the processes running in the domain, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

4. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE`/admin/`domainName`/aserver directory. On Linux, type:

```
IDMHOST1> tar -cvf edgdomainback.tar ORACLE_BASE/admin/domainName/aserver
```

For information about backing up the application tier configuration, see Section 19.4, "Performing Backups and Recoveries."

7

Extending the Domain with Oracle Internet Directory

This chapter describes how to extend the domain with Oracle Internet Directory (OID) in the enterprise deployment.

This chapter includes the following topics:

7.1 Identity Store and Policy Store in Oracle Internet Directory

You use the identity store for storing information about users and groups. You use Policy Store for storing information about security policies and for configuration information. Although you can use a single Oracle Internet Directory instance for storing both the identity and policy information, it is recommended that you use two directory stores.

If you intend to separate your identity and policy information, you must create two highly available instances of Oracle Internet Directory. These instances can coexist on the same nodes or can exist on separate nodes. The data, however, must be stored in two separate databases.

The procedure for installing and configuring the two instances of Oracle Internet Directory is the same. You must, however, point `idstore.mycompany.com` at one of the instances and `policystore.mycompany.com` at the other.

7.2 Prerequisites for Configuring Oracle Identity Directory Instances

Before configuring the Oracle Internet Directory instances on `OIDHOST1` and `OIDHOST2`, ensure that the following tasks have been performed:

1. Synchronize the time on the individual Oracle Internet Directory nodes using Greenwich Mean Time so that there is a discrepancy of no more than 250 seconds between them.

> **Note:** If OID Monitor detects a time discrepancy of more than 250 seconds between the two nodes, the OID Monitor on the node that is behind stops all servers on its node. To correct this problem, synchronize the time on the node that is behind in time. The OID Monitor automatically detects the change in the system time and starts the Oracle Internet Directory servers on its node.

2. Install and upgrade the software on OIDHOST1 and OIDHOST2 as described in Section 4.5.4, "Installing Oracle Identity Management."

3. If you plan on provisioning the Oracle Internet Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on `OIDHOST1` and `OIDHOST2` as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

4. Ensure that the load balancer is configured.

7.3 Configuring the Oracle Internet Directory Instances

Follow these steps to configure the Oracle Internet Directory components, `OIDHOST1` and `OIDHOST2` on the directory tier with Oracle Internet Directory. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

This section contains the following topics:

- Section 7.3.1, "Configuring the First Oracle Internet Directory Instance"
- Section 7.3.2, "Configuring an Additional Oracle Internet Directory Instance"

7.3.1 Configuring the First Oracle Internet Directory Instance

1. Ensure that ports `389` and `636` 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.

   On UNIX:

   ```
   netstat -an | grep "389"
   netstat -an | grep "636"
   ```

   If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

   On UNIX:

   Remove the entries for ports `389` and `636` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

3. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports `389` and `636`, as follows:

   ```
   #The Non-SSL port for OID
   Oracle Internet Directory Port No = 389
   #The SSL port for OID
   Oracle Internet Directory (SSL) Port No = 636
   ```

4. Start the Oracle Identity Management 11*g* Configuration Assistant by running *IDM_ORACLE_HOME*/bin/config.sh on UNIX or *IDM_ORACLE_HOME*\bin\config.bat on Windows.

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

6. On the Select Domain screen, select **Configure without a Domain**.

Click **Next**.

7. On the Specify Installation Location screen, specify the following values:

- Oracle Instance Location: /u01/app/oracle/admin/oid_inst1

- Oracle Instance Name: oid_inst1

Click **Next**.

8. On the Specify Email for Security Updates screen, specify these values:

- Email Address: Provide the email address for your My Oracle Support account.

- Oracle Support Password: Provide the password for your My Oracle Support account.

- Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

9. On the Configure Components screen, select **Oracle Internet Directory**, deselect all the other components, and then click **Next**.

10. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the staticports.ini file that you edited in the temporary directory.

Click **Next**.

11. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:

- Connect String:
  oiddbhost1-vip.mycompany.com:1521:idmdb1^oiddbhost2-vip.my
  company.com:1521:idmdb2@oidedg.mycompany.com

> **Notes:**
>
> - The Oracle RAC database connect string information must be provided in the format:
>
>   `host1`:`port1`:`instance1`^`host2`:`port2`:`instance2`@`servicename`
>
> - During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed. It is required that the information provided is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances. Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.
>
> - If you are using Oracle Database 11.2, replace the `vip` addresses with the 11.2 SCAN address.

- User Name: `ODS`
- Password: `******` (enter the password)

Click **Next**.

12. On the Configure OID screen, specify the Realm and enter the Administrator (`cn=orcladmin`) password and click **Next**.

13. 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. When they are correct, click **Configure**.

14. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

16. To validate the installation of the Oracle Internet Directory instance on `OIDHOST1`, issue these commands:

```
ldapbind -h oidhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oidhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - `ORACLE_HOME`
> - `ORACLE_INSTANCE`
> - `PATH` - The following directory locations should be in your `PATH`:
>
>   - `ORACLE_HOME`/bin
>   - `ORACLE_HOME`/ldap/bin
>   - `ORACLE_HOME`/ldap/admin

It is recommended that you tune Oracle Internet Directory at this point. See the Oracle Internet Directory chapter in the *Oracle Fusion Middleware Performance and Tuning Guide*.

7.3.2 Configuring an Additional Oracle Internet Directory Instance

The schema database must be running before you perform this task. Follow these steps to install Oracle Internet Directory on `OIDHOST2`:

1. Ensure that ports `389` and `636` 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.

   On UNIX:

   ```
   netstat -an | grep "389"
   netstat -an | grep "636"
   ```

   If the ports are in use (that is, if the command returns output identifying either port), you must free them.

   On UNIX:

   Remove the entries for ports `389` and `636` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

3. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom ports:

   ```
   # The non-SSL port for Oracle Internet Directory
   Oracle Internet Directory port = 389
   # The SSL port for Oracle Internet Directory
   Oracle Internet Directory (SSL) port = 636
   ```

4. Start the Oracle Identity Management 11*g* Configuration Assistant by running `IDM_ORACLE_HOME/bin/config.sh`.

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

6. On the Select Domain screen, select **Configure without a Domain**.

   Click **Next**.

7. On the Specify Installation Location screen, specify the following values:

   Oracle Instance Location: `/u01/app/oracle/admin/oid_inst2`

   Oracle Instance Name: `oid_inst2`

   Click **Next**.

8. On the Specify Email for Security Updates screen, specify these values:

   - Email Address: Provide the email address for your My Oracle Support account.

   - Oracle Support Password: Provide the password for your My Oracle Support account.

   - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

9. On the Configure Components screen, select Oracle Internet Directory, deselect all the other components, and click **Next**.

10. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the `staticports.ini` file that you edited in the temporary directory.

Click **Next**.

11. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:

   ▪ Connect String:
   `oiddbhost1-vip.mycompany.com:1521:idmdb1^oiddbhost2-vip.my company.com:1521:idmdb2@oidedg.mycompany.com`

   Notes:

   ▪ The Oracle RAC database connect string information must be provided in the format:

   `host1:port1:instance1^host2:port2:instance2@servicename`

   ▪ During this installation, it is not required that all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.

   ▪ You must provide complete and accurate information. Specifically, you must provide the correct host, port, and instance name for each Oracle RAC instance, and the service name you provide must be configured for all the specified Oracle RAC instances.

   Any incorrect information entered in the Oracle RAC database connect string must be corrected manually after the installation.

   ▪ User Name: `ODS`

   ▪ Password: `******` (enter the password)

   Click **Next**.

12. The ODS Schema in use message appears. The ODS schema chosen is already being used by the existing Oracle Internet Directory instance. Therefore, the new Oracle Internet Directory instance being configured would reuse the same schema.

Choose **Yes** to continue.

A popup window with this message appears:

`"Please ensure that the system time on this Identity Management Node is in sync with the time on other Identity management Nodes that are part of the Oracle Application Server Cluster (Identity Management) configuration. Failure to ensure this may result in unwanted instance failovers, inconsistent operational attributes in directory entries and potential inconsistent behavior of password state policies."`

Ensure that the system time between `IDMHOST1` and `IDMHOST2` is synchronized.

Click **OK** to continue.

13. On the Specify OID Admin Password screen, specify the Oracle Internet Directory administration password and click **Next**.

14. 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. When they are correct, click **Configure**.

15. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

16. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

17. To validate the installation of the Oracle Internet Directory instance on `OIDHOST2`, issue these commands:

```
ldapbind -h oidhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oidhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - `ORACLE_HOME`
>
> - `ORACLE_INSTANCE`
>
> - `PATH` - The following directory locations should be in your `PATH`:
>
>   *ORACLE_HOME*/bin
>
>   *ORACLE_HOME*/ldap/bin
>
>   *ORACLE_HOME*/ldap/admin

7.4 Post-Configuration Steps

Follow the steps in this section to complete the configuration of the Oracle Internet Directory instances.

This section contains the following topics:

- Section 7.4.1, "Registering Oracle Internet Directory with the WebLogic Server Domain"

- Section 7.4.2, "Generating a Certificate to be Used by the Identity Management Domain,"

- Section 7.4.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections"

- Section 7.4.4, "Considering Oracle Internet Directory Password Policies"

7.4.1 Registering Oracle Internet Directory with the WebLogic Server Domain

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Internet Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Internet Directory instances installed on `OIDHOST1` and `OIDHOST2`, follow these steps:

1. Set the `ORACLE_HOME` variable. For example, on `OIDHOST1` and `OIDHOST2`, issue this command:

   ```
   export ORACLE_HOME=IDM_ORACLE_HOME
   ```

2. Set the `ORACLE_INSTANCE` variable. For example:

   On `OIDHOST1`, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/oid_inst1
   ```

   On `OIDHOST2`, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/oid_inst2
   ```

3. Execute the `opmnctl registerinstance` command on both `OIDHOST1` and `OIDHOST2`:

   ```
   ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost WLSHostName -adminPort
   WLSPort -adminUsername adminUserName
   ```

   For example, on OIDHOST1 and OIDHOST2:

   ```
   ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost ADMINVHN -adminPort
   7001 -adminUsername weblogic
   ```

   The command requires login to WebLogic Administration Server (`idmhost1.mycompany.com`)

   Username: `weblogic`

   Password: `*******`

   > **Note:** For additional details on registering Oracle Internet Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance or Component with the WebLogic Server" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

4. Update the Enterprise Manager Repository URL using the emctl utility with the switchOMS flag. The emctl utility is located under the `ORACLE_INSTANCE/EMAGENT/EMAGENT/bin` directory.

   Syntax:

   ```
   ./emctl switchOMS ReposURL.
   ```

   For Example:

   ```
   ./emctl switchOMS http://ADMINVHN:7001/em/upload
   ```

   Output:

   ```
   ./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
   Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
   Copyright (c) 1996, 2009 Oracle Corporation.  All rights reserved.
   SwitchOMS succeeded.
   ```

5. Validate if the agents on `OIDHOST1` and `OIDHOST2` are configured properly to monitor their respective targets. Follow these steps to complete this task:

   ■ Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.

      Log in as the `weblogic` user.

   ■ From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**.

   ■ Validate that the host name in Agent URL under the Agent column matches the host name under the Host column. In case of a mismatch, follow these steps to correct the issue:

      – Click the **configure** link to go to the Configure Target Page.

      – On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

   ■ Update the WebLogic monitoring user name and the WebLogic monitoring password.

      – On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

      – Update the WebLogic monitoring user name and the WebLogic monitoring password. Enter `weblogic` as the WebLogic monitoring user name and the password for the `weblogic` user as the WebLogic monitoring password.

      – Click **OK** to save your changes.

7.4.2 Generating a Certificate to be Used by the Identity Management Domain

Perform this task after you have registered Oracle Internet Directory with Oracle WebLogic Server.

External domains communicate with the Identity Management domain using SSL Server Authentication Only Mode. To enable the Identity Management domain to support this SSL mode, you must generate a certificate and store it in the Policy Store. This adds an extra layer of security, ensuring that only those domains with access to the security certificate can communicate with the domain. The domain level certificate is generated once per domain.

7.4.2.1 Prerequisites

> **Note:** Using the following approach for SSL configuration requires an LDAP server to be available as a central repository and also available as a demoCA. If you are deploying separate instances for Identity Store and Policy Store, you can use the Policy Store Oracle Internet Directory as the store for the SSL repository.

Prior to running this command ensure that:

■ Oracle Identity Management is installed on `IDMHOST1`.

■ Oracle Identity and Access Management is installed on `IDMHOST1`.

- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See http://www.cygwin.com.

> **Note:** When using Cygwin, ensure that you use the "/" character in path names when exporting a variable. For example:
>
> ```
> export ORACLE_HOME=c:/oracle/idm
> ```

7.4.2.2 Generating the Certificate

To generate a certificate for the `IDMDomain` execute the following commands on `IDMHOST1`.

1. Set the `ORACLE_HOME` and `JAVA_HOME` variables. For example, issue this command:

   ```
   export ORACLE_HOME=IDM_ORACLE_HOME
   export PATH=$JAVA_HOME/bin:$PATH
   ```

2. Generate the certificate using the `SSLGenCA` command which is located in `ORACLE_COMMON_HOME`/bin

   For example:

   ```
   cd ORACLE_COMMON_HOME/bin
   ./SSLGenCA.sh
   ```

3. When the command executes supply the following information:

   - LDAP host Name: `policystore.mycompany.com`.

   > **Note:** It is recommended that you use the Policy Store directory, not the Identity Store.

   - LDAP Port: `389`
   - Admin User: `cn=orcladmin`
   - password: `admin_password`
   - LDAP sslDomain where your CA will be stored: `IDMDomain`
   - Password to protect your CA wallet: `wallet_password`
   - Confirmed password for your CA wallet: `wallet_password`

Sample output:

```
SSL Certificate Authority Generation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.

************************************************************************
*********** This tool will generate a self-signed CA wallet ************
*********** and store it in a central LDAP directory ************
*********** for IDM and FA SSL set up and provisioning ************
************************************************************************
>>>Enter the LDAP hostname [slc00xx.mycompany.com]: policystore.mycompany.com
>>>Enter the LDAP port [3060]: 389
>>>Enter the admin user [cn=orcladmin]
>>>Enter password for cn=orcladmin:
```

```
>>>Enter the LDAP sslDomain where your CA will be stored [idm]: IDMDomain
>>>Enter a password to protect your CA wallet:
>>>Enter confirmed password for your CA wallet:

Generate a new CA Wallet...
Create SSL Domains Container for cn=IDMDomain,cn=sslDomains...
Storing the newly generated CA to the LDAP...
Set up ACL to protect the CA wallet...
>>>The newly generated CA is stored in LDAP entry
cn=demoCA,cn=IDMDomain,cn=sslDomains successfully.
```

This script performs the following tasks:

- Creates a Demo Signing CA wallet for use in the domain.

- Extracts the public Demo CA Certificate from the CA wallet.

- Uploads the wallet and the certificate to LDAP and stores them in the entry:
  `cn=demoCA,Deployment_SSL_Domain`

- Creates an access group in LDAP:
  `cn=SSLDomains,cn=IDMDomain,cn=demoCA` and grants that group
  administrative privileges to the parent container. All other entities are denied
  access. Add users to the group to give access. The Demo CA Certificate is now
  available for download by an anonymous or authenticated user.

- The Demo CA Wallet password is stored locally in an obfuscated wallet for future
  use. Its path is: *ORACLE_HOME*/credCA/castore

  As administrator, you must secure this wallet so that only SSL administrators can
  read it.

  The best place to locate the Certificate is in the Policy Store.

7.4.3 Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections

If you plan to enable SSL Server Authentication Only Mode for your domain and have
created a domain level SSL certificate as described in Section 7.4.2, "Generating a
Certificate to be Used by the Identity Management Domain," you must perform the
following to ensure that your Oracle Internet Directory instances are capable of
accepting requests using this mode. You must configure each Oracle Internet Directory
instance independently.

7.4.3.1 Prerequisites

Prior to running this command ensure that:

- Oracle Internet Directory is installed.

- Oracle Identity Management is installed on `IDMHOST1`

- Site certificate has been generated as described in Section 7.4.2, "Generating a
  Certificate to be Used by the Identity Management Domain."

- If you are using Windows, you have installed a UNIX emulation package such as
  Cygwin in order to run the scripts contained in this section. See
  `http://www.cygwin.com.`

7.4.3.2 Configuring Oracle Internet Directory for SSL

To enable Oracle Internet Directory to communicate using SSL Server Authentication Mode, perform the following steps on `OIDHOST1` and `OIDHOST2`:

> **Note:** When you perform this operation, only the Oracle Internet Directory instance you are working on should be running.

1. Set the `ORACLE_HOME`, `ORACLE_INSTANCE` and `JAVA_HOME` variables. For example, on `OIDHOST1`, issue this command

   ```
   export ORACLE_HOME=IDM_ORACLE_HOME
   export ORACLE_INSTANCE=/u01/app/oracle/admin/oid_inst1
   export JAVA_HOME=MW_HOME/jrockit_version
   export PATH=$JAVA_HOME/bin:$PATH
   ```

2. To enable SSL Server Authentication use the tool SSLServerConfig which is located in:

   `ORACLE_COMMON_HOME/bin`

   For example

   ```
   $ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component oid
   ```

3. When prompted, enter the following information:

   - LDAP Hostname: Central LDAP host, for example: `policystore.mycompany.com`

   - LDAP port: LDAP port, for example: `389`

   - Admin user DN: `cn=orcladmin`

   - Password: `administrator_password`

   - sslDomain for the CA: `IDMDomain` Oracle recommends that the SSLDomain name be the same as the Weblogic domain name to make reference easier.

   - Password to protect your SSL wallet/keystore: `password_for_local_keystore`

   - Enter confirmed password for your SSL wallet/keystore: `password_for_local_keystore`

   - Password for the CA wallet: `certificate_password`. This is the one created in Section 7.4.2, "Generating a Certificate to be Used by the Identity Management Domain."

   - Country Name 2 letter code: Two letter country code, such as `US`

   - State or Province Name: State or province, for example: `California`

   - Locality Name: Enter the name of your city, for example: `RedwoodCity`

   - Organization Name: Company name, for example: `mycompany`

   - Organizational Unit Name: Leave at the default

   - Common Name: Name of this host, for example: `OIDHOST1.mycompany.com`

   - OID component name: Name of your Oracle Instance, for example: `oid1`

- WebLogic admin host: Host running the WebLogic Administration Server, for example:. `adminvhn.mycompany.com`

- WebLogic admin port: WebLogic Administration Server port, for example: `7001`

- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`

- WebLogic password: `password`.

- AS instance name: Name of your Oracle instance, for example: `oid1`

- SSL wallet name for OID component [oid_wallet1]: Accept the default

- Do you want to restart your OID component: `Yes`

- Do you want to test your SSL setup? `Yes`

- SSL Port of your OID Server: `389`

Sample output:

```
Server SSL Automation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.

Downloading the CA wallet from the central LDAP location...
>>>Enter the LDAP Hostname [slc00dra.us.oracle.com]: policystore.mycompany.com
>>>Enter the LDAP port [3060]: 389
>>>Enter an admin user DN [cn=orcladmin]
>>>Enter password for cn=orcladmin:
>>>Enter the sslDomain for the CA [idm]: IDMDomain
>>>Enter a password to protect your SSL wallet/keystore:
>>>Enter confirmed password for your SSL wallet/keystore:
>>>Enter password for the CA wallet:
>>>Searching the LDAP for the CA usercertificate ...
Importing the CA certifcate into trust stores...
>>>Searching the LDAP for the CA userpkcs12 ...

Invoking OID SSL Server Configuration Script...
Enter attribute values for your certificate DN
>>>Country Name 2 letter code [US]:
>>>State or Province Name [California]:
>>>Locality Name(eg, city) []:Redwood
>>>Organization Name (eg, company) [mycompany]:
>>>Organizational Unit Name (eg, section) [oid-20110524015634]:
>>>Common Name (eg, hostName.domainName.com) [slc00xxx.mycompany.com]:
The subject DN is
cn=slc00dra.us.oracle.com,ou=oid-20110524015634,l=Redwood,st=California,c=US

Creating an Oracle SSL Wallet for oid instance...
/u01/app/oracle/product/fmw/IDM/../oracle_common/bin
>>>Enter your OID component name: [oid1]
>>>Enter the weblogic admin server host [slc00xxx.mycompany.com] mdrv1
>>>Enter the weblogic admin port: [7001]
>>>Enter the weblogic admin user: [weblogic]
>>>Enter weblogic password:
>>>Enter your AS instance name:[asinst_1] oid1
>>>Enter an SSL wallet name for OID component [oid_wallet1]
Checking the existence of oid_wallet1 in the OID server...
Configuring the newly generated Oracle Wallet with your OID component...
Do you want to restart your OID component?[y/n]y

Do you want to test your SSL set up?[y/n]y
```

```
>>>Please enter your OID ssl port:[3131] 636
Please enter the OID hostname:[slc00dra.us.oracle.com]
idstore.mycompany.com
>>>Invoking /u01/app/oracle/product/fmw/IDM/bin/ldapbind -h idstore.mycompany.com
-p 636 -U 2 -D cn=orcladmin ...
Bind successful

Your oid1 SSL server has been set up successfully
```

Confirm that the script has been successful.

Repeat all the steps in this section, Section 7.4.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections," for each Oracle Internet Directory instance.

7.4.4 Considering Oracle Internet Directory Password Policies

By default, Oracle Internet Directory passwords expire in 120 days. Users who do not reset their passwords before expiration can no longer authenticate to Oracle Internet Directory. This includes administrative users, such as `oimadminuser`, `oamsoftwareuser`, and `oamadminuser`. Your Identity Management environment cannot work properly unless these users can authenticate. See *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for information about changing Oracle Internet Directory password policies.

7.5 Validating the Oracle Internet Directory Instances

To validate the Oracle Internet Directory instances, ensure that you can connect to each Oracle Internet Directory instance and the load balancing router using these commands:

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - `ORACLE_HOME`
>
> - `ORACLE_INSTANCE`
>
> - `PATH` - The following directory locations should be in your `PATH`:
>
>   *ORACLE_HOME*/bin
>
>   *ORACLE_HOME*/ldap/bin
>
>   *ORACLE_HOME*/ldap/admin

```
ldapbind -h oidhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oidhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oidhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oidhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h policystore.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h policystore.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

If your identity store is also in Oracle Internet Directory then check:

```
ldapbind -h idstore.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h idstore.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

> **Note:** The -q option prompts the user for a password. LDAP tools have been modified to disable the options -w *password* and -P *password* when the environment variable LDAP_PASSWORD_ PROMPTONLY is set to TRUE or 1. Use this feature whenever possible.

7.6 Tuning Oracle Internet Directory

After you deploy Oracle Internet Directory, you must tune it as described in *Oracle Fusion Middleware Performance and Tuning Guide*.

In particular, set the following values when deploying Oracle Identity Management for Fusion Applications:

Attribute	Value
orclskiprefinsql	1
orclmaxcc	4
orclserverprocs	4
orclmatchdnenabled	0
orclmaxldapconns	4096

7.7 Backing up the Oracle Internet Directory Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or at a logical point. Create a backup of the installation after verifying that the install 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. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the Oracle Internet Directory instances in the directory tier:

    a. Shut down the instance using opmnctl located under the *ORACLE_ INSTANCE*/bin directory:

    ORACLE_INSTANCE/bin/opmnctl stopall

    b. Create a backup of the Middleware home on the directory tier. On Linux, as the root user, type:

    tar -cvpf *BACKUP_LOCATION*/dirtier.tar *MW_HOME*

    c. Create a backup of the Instance home on the directory tier as the root user:

    tar -cvpf *BACKUP_LOCATION*/instance_backup.tar *ORACLE_INSTANCE*

    d. Start up the instance using opmnctl located under the *ORACLE_ INSTANCE*/bin directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager.

3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the *ORACLE_ BASE*/admin/domainName/aserver directory. On Linux, type:

    ```
    IDMHOST1> tar cvf edgdomainback.tar ORACLE_BASE/admin/domainName/aserver
    ```

    > **Note:**   Create backups on all machines in the directory tier by following the steps shown in this section.
    >
    > For more information about backing up the directory tier configuration, see Section 19.4, "Performing Backups and Recoveries."

8

Extending the Domain with Oracle Directory Integration Platform and ODSM

Oracle Directory Integration Platform is a Java EE application that enables you to integrate your applications and directories, including third-party LDAP directories, with Oracle Internet Directory.

Oracle Directory Integration Platform includes services and interfaces that allow you to deploy synchronization solutions with other enterprise repositories. It can also be used to provide Oracle Internet Directory interoperability with third party metadirectory solutions.

Oracle Directory Services Manager is a unified graphical user interface (GUI) for managing instances of Oracle Internet Directory and Oracle Virtual Directory. Oracle Directory Services Manager enables you to configure the structure of the directory, define objects in the directory, add and configure users, groups, and other entries.

This chapter describes how to install and configure Oracle Directory Integration Platform (DIP) and Oracle Directory Services Manager (ODSM).

Oracle Directory Integration Platform is an optional product. If it is not required in your environment, do not configure it.

This chapter includes the following topics:

- Section 8.1, "Extending the Oracle WebLogic Domain with Oracle Directory Integration Platform and ODSM"

- Section 8.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster"

- Section 8.3, "Provisioning the Managed Servers on the Local Disk"

- Section 8.4, "Configuring ODSM to work with the Oracle Web Tier"

- Section 8.5, "Validating the Application Tier Configuration"

- Section 8.6, "Backing Up the Application Tier Configuration"

8.1 Extending the Oracle WebLogic Domain with Oracle Directory Integration Platform and ODSM

The application tier consists of multiple computers hosting the Oracle Directory Integration Platform, Oracle Directory Services Manager, and Oracle Access Manager instances. In the complete configuration, requests are balanced among the instances on the application tier computers to create a high-performing, fault tolerant application environment.

> **Note:** Oracle Directory Integration Platform uses Quartz to maintain its jobs and schedules in the database. For the Quartz jobs to be run on different Oracle Directory Integration Platform nodes in a cluster, it is recommended that the system clocks on the cluster nodes be synchronized.

Follow these steps to install and configure Oracle Directory Integration Platform and Oracle Directory Services Manager on IDMHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

3. Ensure that port 7006 is 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.

   On UNIX:

   ```
   netstat -an | grep "7006"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   On UNIX:

   Remove the entries for port 7006 in the /etc/services file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

4. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

5. Copy the staticports.ini file from the Disk1/stage/Response directory to a temporary directory.

6. Edit the staticports.ini file that you copied to the temporary directory to assign the following custom port:

   ```
   # The port for ODSM Server port
   ODS Server Port No = 7006
   ```

7. Start the Oracle Identity Management 11*g* Configuration Assistant by running the config.sh script located under the *ORACLE_HOME*/bin directory on IDMHOST1. For example:

   ```
   /u01/app/oracle/product/fmw/idm/bin/config.sh
   ```

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

9. On the Select Domain screen, select **Extend Existing Domain** and enter the domain details:

- **Hostname**: `ADMINVHN.mycompany.com`

- **Port**: 7001

- **User Name:** `weblogic`

- **User Password:** *user password*

Click **Next**.

10. A dialog box with the following message appears:

```
The selected domain is not a valid Identity Management domain or the installer
cannot determine if it is a valid domain. If you created the domain using the
Identity Management installer, you can ignore this message and continue. If
you did not create the domain using the Identity Management installer, refer
to the Identity Management documentation for information on how to verify the
domain is valid.
```

Click **Yes** to continue.

This is a benign warning that you can ignore.

11. On the Specify Installation Location screen, specify the following values (the values for the **Oracle Middleware Home Location** and the **Oracle Home Directory** fields are prefilled. The values default to the Middleware home and Oracle home previously installed on IDMHOST1 in Section 6.1, "Enabling ADMINVHN on IDMHOST1":

- **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`

- **Oracle Home Directory**: `idm`

- **WebLogic Server Directory**: `/u01/app/oracle/product/fmw/wlserver_10.3`

- **Oracle Instance Location:** `/u01/app/oracle/admin/ods_inst1`

- **Oracle Instance Name**: `ods_inst1`

Click **Next**.

12. On the Specify Email for Security Updates screen, specify these values:

- **Email Address**: Provide the email address for your My Oracle Support account.

- **Oracle Support Password**: Provide the password for your My Oracle Support account.

- Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

13. On the Configure Components screen, select the following components:

- **Oracle Directory Integration Platform**

- **Management Components - Oracle Directory Services Manager**

Deselect all the other components.

Select the **Clustered** check box.

Click **Next**.

14. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the `staticports.ini` file that you edited in the temporary directory

    Click **Next**.

15. On the Specify OID Details screen, specify the following:

    - **Hostname:** `idstore.mycompany.com`
    - **SSL_Port**: `636`
    - **Username:** `cn=orcladmin`
    - **Password:** `******`

    Click **Next**.

16. On the Specify Schema Database screen, specify the following values:

    - Connect String:

      ```
      oiddbhost1-vip.mycompany.com:1521:idmdb1^oiddbhost2-vip.mycompany.com:1521:
      idmdb2@oidedg.mycompany.com
      ```

      Notes:

      - The Oracle RAC database connect string information must be provided in the format:

        host1:port1:instance1^host2:port2:instance2@servicename

      - During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.

      - It is required that the information provided is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances.

        Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.

      - If you are using Oracle Database 11.2, replace the `vip` addresses with the 11.2 SCAN address.

    - User Name: `ODSSM`
    - Password: `******`

    Click **Next**.

17. 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), and click **Configure**.

18. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.

19. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

8.2 Expanding the Oracle Directory Integration Platform and ODSM Cluster

This section includes the steps for extending the WebLogic Server Domain on IDMHOST2.

This section contains the following topics:

8.2.1 Installing and Configuring Oracle Directory Integration Platform and ODSM on IDMHOST2

Follow these steps to install and configure Oracle Directory Integration Platform and Oracle Directory Service Manager on IDMHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST2 as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

3. Ensure that port number 7006 is not in use by any service on the computer by issuing this command for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "7006"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   On UNIX:

   Remove the entries for port 7006 in the `/etc/services` file if the port is in use by a service and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

4. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

5. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

   ```
   #The port for ODSM Server port
   ODS Server Port No: 7006
   ```

6. Start the Oracle Identity Management 11g Configuration Assistant by running the `config.sh` script located under the *ORACLE_HOME*/bin directory on IDMHOST2. For example:

   ```
   /u01/app/oracle/product/fmw/idm/bin/config.sh
   ```

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

8. On the Select Domain screen, select the **Expand Cluster** option and specify these values:

   ■ **Hostname**: `ADMINVHN.mycompany.com`

   ■ **Port**: `7001`

   ■ **UserName**: `weblogic`

   ■ **User Password**: *password for the webLogic user*

   Click **Next**.

9. A dialog box with the following message appears:

   ```
   The selected domain is not a valid Identity Management domain or the installer
   cannot determine if it is a valid domain. If you created the domain using the
   Identity Management installer, you can ignore this message and continue. If you
   did not create the domain using the Identity Management installer, refer to the
   Identity Management documentation for information on how to verify the domain
   is valid.
   ```

   Click **OK** to continue.

   This is a benign warning that you can safely ignore.

10. On the Specify Installation Location screen, specify the following values. The values for the **Oracle Middleware Home Location** and the **Oracle Home Directory** fields are prefilled. The values default to the Middleware home and Oracle home previously installed on `IDMHOST1` in Section 6.1, "Enabling ADMINVHN on IDMHOST1."

    ■ **Oracle Middleware Home Location**: `/u01/app/oracle/product/fmw`

    ■ **Oracle Home Directory**: idm

    ■ **WebLogic Server Directory**: `/u01/app/oracle/product/fmw/wlserver_10.3`

    ■ **Oracle Instance Location**: `/u01/app/oracle/admin/ods_inst2`

    ■ **Oracle Instance Name**: `ods_inst2`

    Click **Next**.

11. On the Email for Security Updates screen, specify these values:

    ■ **Email Address**: Provide the email address for your My Oracle Support account.

    ■ **Oracle Support Password**: Provide the password for your My Oracle Support account.

    ■ Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.

12. On the Configure Components screen, de-select all the products except **Oracle DIP and Management Components** and then click **Next**.

13. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the `staticports.ini` file that you edited in the temporary directory.

    Click **Next**.

14. 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), and click **Configure**.

15. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.

16. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

8.2.2 Post-Installation Step: Copying Oracle Directory Integration Platform to wls_ods2

Ignore this section if you are not using Oracle Directory Integration Platform.

In the previous section, the installer created a second Managed Server, `WLS_ODS2` on `IDMHOST2`. However, the Oracle Directory Integration Platform application is not deployed to the `WLS_ODS2` Managed Server.

To complete the installation and configuration of the Oracle Directory Integration Platform and Oracle Directory Services Manager applications on `IDMHOST2`, proceed as follows:

On `IDMHOST1`, copy the `ORACLE_BASE`/admin/IDMDomain/aserver/`IDMDomain`/config/fmwconfig/servers/ wls_ods1/applications directory to the `ORACLE_BASE`/admin/`IDMDomain`/aserver/`IDMDomain`/config/fmwconfig/servers/ wls_ods2 directory on `IDMHOST2`. For example:

```
cp -rp ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_
ods1/applications  ORACLE_
BASE/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_
ods2/applications
```

During `wls_ods2` startup, the application is automatically propagated to `IDMHOST2`.

8.2.3 Configure the Enterprise Manager Agents

All the Oracle Fusion Middleware components deployed in this enterprise are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage DIP and ODSM with this tool, you must configure the EM agents with the correct monitoring credentials. Follow these steps to complete this task:

1. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`. Log in as the `weblogic` user.

2. From the Domain Home Page, navigate to the Agent-Monitored Targets page using the menu under **Farm -> Agent-Monitored Targets**.

   - Click the **Configure** link to go to the Configure Target Page.

   - On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

   - Update the **WebLogic monitoring user name** and the **WebLogic monitoring password**. Enter `weblogic` as the **WebLogic monitoring user name** and the password for the `weblogic` user as the **WebLogic monitoring password**.

   - Click **OK** to save your changes.

8.3 Provisioning the Managed Servers on the Local Disk

This section provides the steps to provision the Managed Server on the local disk. Proceed as follows:

1. Stop the ODS instances on both IDMHOST1 and IDMHOST2. Follow the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components"

2. On IDMHOST1, pack the Managed Server domain using the pack command located under the *ORACLE_COMMON_HOME*/common/bin directory. Make sure to pass managed=-true flag to pack the Managed Server. Type:

    ```
    ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
        -domain=path_to_adminServer_domain -template=templateName.jar \
        -template_name=templateName
    ```

    For example

    ```
    ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
      -domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain \
      -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
      -template_name=ManagedServer_Template
    ```

3. Unpack the Managed Server to the local disk on IDMHOST1 using the unpack command located under the *ORACLE_COMMON_HOME* /common/bin directory.

    ```
    ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
        -template=templateName.jar -app_dir=path_to_appdir_on_localdisk
    ```

    For example:

    ```
    ORACLE_COMMON_HOME/common/bin/unpack.sh \
        -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
        -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
        -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
    ```

4. Copy the Managed Server template directory from IDMHOST1 to IDMHOST2. For Example:

    ```
    scp -rp /u01/app/oracle/products/fmw/templates
    user@IDMHOST2:/u01/app/oracle/products/fmw/templates
    ```

5. Unpack the Managed Server to the local disk on IDMHOST2 using the unpack command located under the *ORACLE_HOME*/common/bin directory.

    ```
    ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
        -template=templateName.jar -app_dir=path_to_appdir_on_localdisk
    ```

    For example:

    ```
    ORACLE_COMMON_HOME/common/bin/unpack.sh \
        -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
        -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
        -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
    ```

6. Stop and Start the Managed Servers instances as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

7. Start the ODS instances on both IDMHOST1 and IDMHOST2. Follow the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

8. Delete the *ORACLE_BASE*/admin/IDMDomain/aserver/IDMDomain/servers/wls_ods1

directory on `IDMHOST1` and the *ORACLE_BASE*/admin/IDMDomain/aserver/IDMDomain/servers/wls_ods2 directory on `IDMHOST2`.

These directories are created by the Oracle Universal Installer when the domain is originally configured and are no longer required after the provisioning the Managed Server to the local disk.

8.4 Configuring ODSM to work with the Oracle Web Tier

This section describes how to configure Oracle Directory Services Manager to work with the Oracle Web Tier.

This section contains the following topics:

- Section 8.4.1, "Prerequisites"
- Section 8.4.2, "Configuring Oracle HTTP Servers to Access the ODSM Console"

8.4.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on `WEBHOST1` and `WEBHOST2`.

2. Install and configure ODSM and Oracle Directory Integration Platform on `IDMHOST1` and `IDMHOST2`.

3. Configure the load balancer with a virtual host name (`admin.mycompany.com`) pointing to web servers `WEBHOST1` and `WEBHOST2`.

8.4.2 Configuring Oracle HTTP Servers to Access the ODSM Console

On each of the web servers on `WEBHOST1` and `WEBHOST2`, a file called `admin.conf` was created in the directory *ORACLE_INSTANCE*/config/OHS/component/moduleconf, as described Section 6.9, "Configuring Oracle HTTP Server for the WebLogic Administration Server." Edit this file and add the following lines within the virtual host definition:

```
<Location /odsm>
   SetHandler weblogic-handler
   WebLogicCluster idmhost1.mycompany.com:odsm_port1,idmhost2.mycompany.com:odsm_port2
 </Location>
```

After editing the file should look like this:

```
NameVirtualHost *:80

<VirtualHost *:80>

   ServerName admin.mycompany.com:80
   ServerAdmin you@your.address
   RewriteEngine On
   RewriteOptions inherit

   # Admin Server and EM
   <Location /console>
     SetHandler weblogic-handler
     WebLogicHost ADMINVHN
     WeblogicPort 7001
```

```
   </Location>

   <Location /consolehelp>
      SetHandler weblogic-handler
      WebLogicHost ADMINVHN
      WeblogicPort 7001
   </Location>

   <Location /em>
      SetHandler weblogic-handler
      WebLogicHost ADMINVHN
      WeblogicPort 7001
   </Location>

   <Location /odsm>
      SetHandler weblogic-handler
      WebLogicCluster idmhost1.mycompany.com:odsm_
port1,idmhost2.mycompany.com:odsm_port2
   </Location>

</VirtualHost>
```

Restart the Oracle HTTP Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

8.5 Validating the Application Tier Configuration

This section includes steps for validating Oracle Directory Services Manager and Oracle Directory Integration Platform.

This section contains the following topics:

- Section 8.5.1, "Validating Oracle Directory Services Manager"
- Section 8.5.2, "Validating Oracle Directory Integration Platform"

8.5.1 Validating Oracle Directory Services Manager

Follow these steps to validate the Oracle Directory Services Manager installation:

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://hostname.mycompany.com:port/odsm`

   For example, on `IDMHOST1`, enter this URL:

   `http://idmhost1.mycompany.com:7006/odsm`

   and on `IDMHOST2`, enter this URL:

   `http://idmhost2.mycompany.com:7006/odsm`

2. Access ODSM through the load balancer address:
   `http://admin.mycompany.com/odsm`

3. Validate that Oracle Directory Services Manager can create connections to Oracle Internet Directory. Follow these steps to create connections to Oracle Internet Directory:

   To create connections to Oracle Internet Directory, create a connection to the Oracle Internet Directory on each ODSM instance separately. Even though ODSM is clustered, the connection details are local to each node. Proceed as follows:

   a. Launch Oracle Directory Services Manager from IDMHOST1:

```
http://idmhost1.mycompany.com/odsm
```

   b. Create a connection to the Oracle Internet Directory virtual host by providing the following information in ODSM:

Host: `oid.mycompany.com`

Port: `636`

Enable the SSL option

User: `cn=orcladmin`

Password: `ldap-password`

   c. Launch Oracle Directory Services Manager from `IDMHOST2`. Follow Step b to create a connection to Oracle Internet Directory from `IDMHOST2`

> **Note:** Accept the certificate when prompted.

8.5.2 Validating Oracle Directory Integration Platform

Validate the Oracle Directory Integration Platform installation by using the WLST `dipStatus` command. To run this command, follow these steps:

1. Set the `ORACLE_HOME` environment variable to the directory where you installed the Identity Management binaries. For example:

```
export ORACLE_HOME=/u01/app/oracle/product/fmw/idm
```

2. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server. For example:

```
export WLS_HOME=/u01/app/oracle/product/fmw/wlserver_10.3
```

3. Run the `ORACLE_HOME/bin/dipStatus -h hostName -p port -D wlsuser` command.

For example, on `IDMHOST1`, the command and output look like this:

```
ORACLE_HOME/bin/dipStatus -h idmhost1.mycompany.com -p 7006 -D weblogic
[Weblogic user password]
Connection parameters initialized.
Connecting at idmhost1.mycompany.com:7006, with userid "weblogic"..
Connected successfully.

ODIP Application is active at this host and port.
```

For example, on IDMHOST2, the command and output look like this:

```
ORACLE_HOME/bin/dipStatus -h idmhost2.mycompany.com -p 7006 -D weblogic
[Weblogic user password]
Connection parameters initialized.
Connecting at idmhost2.mycompany.com:7006, with userid "weblogic"..
Connected successfully.

ODIP Application is active at this host and port.
```

8.6 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 5.5, "Backing up the Web Tier Configuration."

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 application tier instances by following these steps:

    a. Shut down the instance using `opmnctl` located under the *ORACLE_INSTANCE*/`bin` directory:

       `ORACLE_INSTANCE`/bin/opmnctl stopall

    b. Create a backup of the Middleware home on the application tier. On Linux, as the `root` user, type:

       tar -cvpf `BACKUP_LOCATION`/apptier.tar `ORACLE_BASE`

    c. Create a backup of the Instance home on the application tier as the `root` user:

       tar -cvpf `BACKUP_LOCATION`/instance_backup.tar `ORACLE_INSTANCE`

    d. Start up the instance using `opmnctl` located under the *ORACLE_INSTANCE*/`bin` directory:

       `ORACLE_INSTANCE`/bin/opmnctl startall

4. Back up the Administration Server domain directory as described in Section 6.15, "Backing Up the WebLogic Domain."

5. Back up the Oracle Internet Directory as described in Section 7.7, "Backing up the Oracle Internet Directory Configuration."

For information about backing up the application tier configuration, see Section 19.4, "Performing Backups and Recoveries."

9

Extending the Domain with Oracle Virtual Directory

This chapter describes how to extend the domain with Oracle Virtual Directory (OVD) in the enterprise deployment.

This chapter includes the following topics:

- Section 9.1, "Prerequisites for Configuring Oracle Virtual Directory Instances"
- Section 9.2, "When to use Oracle Virtual Directory"
- Section 9.3, "Configuring the Oracle Virtual Directory Instances"
- Section 9.4, "Post-Configuration Steps"
- Section 9.5, "Disable Oracle Virtual Directory Listener SSL NIO"
- Section 9.6, "Validating the Oracle Virtual Directory Instances"
- Section 9.7, "Creating ODSM Connections to Oracle Virtual Directory"
- Section 9.8, "Creating Adapters in Oracle Virtual Directory"
- Section 9.9, "Tuning Oracle Virtual Directory"
- Section 9.10, "Backing Up the Oracle Virtual Directory Configuration"

Follow these steps to configure the Oracle Virtual Directory components, `OVDHOST1` and `OVDHOST2` on the directory tier with Oracle Virtual Directory. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

9.1 Prerequisites for Configuring Oracle Virtual Directory Instances

Before configuring the Oracle Virtual Directory instances on `OVDHOST1` and `OVDHOST2`, ensure that the following tasks have been performed:

1. Install and upgrade the software on `OVDHOST1` and `OVDHOST2` as described in the following sections.

2. If you plan on provisioning the Oracle Virtual Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on `OVDHOST1` and `OVDHOST2` as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

3. Ensure that the load balancer is configured as describe in Section 2.2.2, "Configuring Virtual Server Names and Ports on the Load Balancer."

9.2 When to use Oracle Virtual Directory

Use Oracle Virtual Directory if any of the following conditions is true:

- Identity Information is not stored in Oracle Internet Directory.

- Identity Information is stored in multiple directories.

- You have decided to standardize on the use of Oracle Virtual Directory.

If your implementation using Oracle Internet Directory exclusively, and your identity data is stored in a single internet directory, then you do not need to use Oracle Virtual Directory.

9.3 Configuring the Oracle Virtual Directory Instances

This section contains the following topics:

- Section 9.3.1, "Configuring the First Oracle Virtual Directory Instance"

- Section 9.3.2, "Configuring an Additional Oracle Virtual Directory"

9.3.1 Configuring the First Oracle Virtual Directory Instance

1. Ensure that ports `6501` and `7501` 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.

   On UNIX:

   ```
   netstat -an | grep "6501"
   netstat -an | grep "7501"
   ```

   If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

   On UNIX:

   Remove the entries for ports `6501` and `7501` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

3. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports `6501` and `7501`, as follows:

   ```
   # The non-SSL port for Oracle Virtual Directory
   Oracle Virtual Directory port = 6501
   # The SSL port for Oracle Virtual Directory
   Oracle Virtual Directory (SSL) port = 7501
   ```

4. Start the Oracle Identity Management 11*g* Configuration Assistant by running `IDM_ORACLE_HOME`/bin/config.sh.

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

6. On the Select Domain screen, select **Configure without a Domain**.

   Click **Next**.

7. On the Specify Installation Location screen, specify the following values:

   - Oracle Instance Location: `/u01/app/oracle/admin/ovd_inst1`

- Oracle Instance Name: `ovd_inst1`

   Click **Next**.

8. On the Specify Email for Security Updates screen, specify these values:

   - Email Address: Provide the email address for your My Oracle Support account.

   - Oracle Support Password: Provide the password for your My Oracle Support account.

   - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

   Click **Next**.

9. On the Configure Components screen, select **Oracle Virtual Directory**, deselect all the other components, and then click **Next**.

10. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the `staticports.ini` file that you edited in the temporary directory.

    Click **Next**.

11. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

    - LDAP v3 Name Space: `dc=mycompany,dc=com`

    In the OVD Administrator section, enter:

    - Administrator User Name: `cn=orcladmin`

    - Password: *administrator_password*

    - Confirm Password: *administrator_password*

    Select **Configure the Administrative Server in secure mode**.

    Click **Next**.

12. 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. When they are correct, click **Configure**.

13. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

    Click **Next**.

14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

15. To validate the installation of the Oracle Virtual Directory instance on `OVDHOST1`, issue these commands:

```
ldapbind -h ovdhost1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - `ORACLE_HOME`
>
> - `ORACLE_INSTANCE`
>
> - `PATH` - The following directory locations should be in your `PATH`:
>
>   *ORACLE_HOME*`/bin`
>
>   *ORACLE_HOME*`/ldap/bin`
>
>   *ORACLE_HOME*`/ldap/admin`

9.3.2 Configuring an Additional Oracle Virtual Directory

The schema database must be running before you perform this task. Follow these steps to install Oracle Virtual Directory on `OVDHOST2`:

1. Ensure that ports `6501` and `7501` 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.

    On UNIX:

    ```
    netstat -an | grep "6501"
    netstat -an | grep "7501"
    ```

2. If the ports are in use (that is, if the command returns output identifying either port), you must free them.

3. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

    On UNIX, remove the entries for ports `6501` and `7501` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

4. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom ports:

    ```
    # The non-SSL port for Oracle Virtual Directory
    Oracle Virtual Directory port = 6501
    # The SSL port for Oracle Virtual Directory
    Oracle Virtual Directory (SSL) port = 7501
    ```

5. Start the Oracle Identity Management 11*g* Configuration Assistant by running *IDM_ORACLE_HOME*`/bin/config.sh`.

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

7. On the Select Domain screen, select **Configure without a Domain**.

    Click **Next**.

8. On the Specify Installation Location screen, specify the following values:

    Oracle Instance Location: `/u01/app/oracle/admin/ovd_inst2`

    Oracle Instance Name: `ovd_inst2`

    Click **Next**.

9. On the Specify Email for Security Updates screen, specify these values:

- **Email Address**: Provide the email address for your My Oracle Support account.

- **Oracle Support Password**: Provide the password for your My Oracle Support account.

- Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

10. On the Configure Components screen, select Oracle Virtual Directory, deselect all the other components, and click **Next**.

11. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full path name to the staticports.ini file that you edited in the temporary directory.

    Click **Next**.

12. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

    - LDAP v3 Name Space: dc=mycompany,dc=com

    In the OVD Administrator section, enter:

    - Administrator User Name: cn=orcladmin

    - Password: *administrator_password*

    - Confirm Password: *administrator_password*

    Select **Configure the Administrative Server in secure mode**.

    Click **Next**.

13. 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. When they are correct, click **Configure**.

14. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

    Click **Next**.

15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

16. To validate the installation of the Oracle Virtual Directory instance on OVDHOST2, issue these commands:

```
ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

> **Note:** Ensure that the following environment variables are set before using `ldapbind`:
>
> - `ORACLE_HOME`
>
> - `ORACLE_INSTANCE`
>
> - `PATH` - The following directory locations should be in your `PATH`:
>
>   *ORACLE_HOME*`/bin`
>
>   *ORACLE_HOME*`/ldap/bin`
>
>   *ORACLE_HOME*`/ldap/admin`

9.4 Post-Configuration Steps

This section contains the following topics:

9.4.1 Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Virtual Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Virtual Directory instances, follow these steps on: `OVDHOST2` and `OVDHOST2`.

1. Set the `ORACLE_HOME` variable. For example, issue this command:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/fmw/idm
   ```

2. Set the `ORACLE_INSTANCE` variable. For example, on `OVDHOST1`, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd_inst1
   ```

   On `OVDHOST2`, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd_inst2
   ```

3. Execute the `opmnctl registerinstance` command:

   ```
   ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost WLSHostName -adminPort
   WLSPort -adminUsername adminUserName
   ```

   For example:

   ```
   ORACLE_INSTANCE/bin/opmnctl registerinstance \
       -adminHost ADMINVHN.mycompany.com -adminPort 7001 -adminUsername weblogic
   ```

   The command requires login to WebLogic Administration Server.

Username: `weblogic`

Password: `password`

> **Note:** For additional details on registering Oracle Virtual Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance Using OPMNCTL" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

4. Update the Enterprise Manager Repository URL using the `emctl` utility with the `switchOMS` flag. The `emctl` utility is located under the *ORACLE_INSTANCE*/EMAGENT/EMAGENT/bin directory.

   Syntax:

   ```
   /emctl switchOMS ReposURL
   ```

   For Example:

   ```
   /emctl switchOMS http://ADMINVNH:7001/em/upload
   ```

   Output:

   ```
   ./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
   Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
   Copyright (c) 1996, 2009 Oracle Corporation.  All rights reserved.
   SwitchOMS succeeded.
   ```

5. Validate if the agents on `OVDHOST1` and `OVDHOST2` are configured properly to monitor their respective targets. Follow these steps to complete this task:

   a. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://adminvhn.mycompany.com:7001/em`. Log in as the weblogic user.

   b. From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**

   c. Validate that the host name in Agent URL under the Agent column matches the host name under the Host column. In case of a mismatch follow these steps to correct the issue:

      – Click **configure** to go to the Configure Target Page.

      – On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

      – Update the WebLogic monitoring user name and the WebLogic monitoring password. Enter `weblogic` as the WebLogic monitoring user name and the password for the weblogic user as the WebLogic monitoring password.

      – Click **OK** to save your changes.

9.4.2 Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections

Configure Oracle Virtual Directory as follows.

9.4.2.1 Prerequisites

Prior to running this command ensure that:

- Oracle Identity Management is installed

- Oracle Identity and Access Management is installed.

- Site certificate has been generated as described in Section 7.4.2, "Generating a Certificate to be Used by the Identity Management Domain."

- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See `http://www.cygwin.com`.

9.4.2.2 Configuring Oracle Virtual Directory for SSL

Before configuring Oracle Virtual Directory for SSL, set the `ORACLE_HOME`, `ORACLE_INSTANCE` and `JAVA_HOME` variables. For example, on `OVDHOST1` and `OVDHOST2`, issue this command

```
export ORACLE_HOME=IDM_ORACLE_HOME
export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd_inst1
export PATH=$JAVA_HOME/bin:$PATH
```

Start the SSL Configuration tool by issuing the command `SSLServerConfig` command which is located in the directory `ORACLE_COMMON_HOME`/bin directory.

For example:

```
ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component ovd
```

When prompted, enter the following information:

- LDAP Hostname: Central LDAP host, for example: `policystore.mycompany.com`

> **Note:** It is recommended that you use the Policy Store directory, not the Identity Store.

- LDAP port: LDAP port, for example: `389`

- Admin user DN: `cn=orcladmin`

- Password: `administrator_password`

- sslDomain for the CA: `IDMDomain`

- Password to protect your SSL wallet/keystore: `password_for_local_keystore`

- Enter confirmed password for your SSL wallet/keystore: `password_for_local_keystore`

- Password for the CA wallet: `certificate_password`. This is the one created in Section 7.4.2, "Generating a Certificate to be Used by the Identity Management Domain."

- Country Name 2 letter code: Two letter country code, such as `US`

- State or Province Name: State or province, for example: `California`

- Locality Name: Enter the name of your city, for example: `RedwoodCity`

- Organization Name: Company name, for example: `mycompany`

- Organizational Unit Name: Leave at the default

- Common Name: Name of this host, for example: `OVDHOST1.mycompany.com`

- OVD component name: Name of your Oracle Instance, for example: `ovd1`

- OVD Component Name: for example, `ovd1`

- AS instance name: Name of your Oracle instance, for example: `asinst_ovd1`

- WebLogic admin host: Host running the WebLogic Administration Server, for example:. `adminvhn.mycompany.com`

- WebLogic admin port: WebLogic Administration Server port, for example: `7001`

- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`

- WebLogic password: `password`.

- SSL wallet name for OVD component [ovdks1.jks]: Accept the default

When asked if you want to restart your Oracle Virtual Directory component, enter `Yes`.

When asked if you would like to test your OVD SSL connection, enter `Yes`. Ensure that the test is a success.

9.5 Disable Oracle Virtual Directory Listener SSL NIO

Before you can bind to the SSL port on Oracle Virtual Directory you must disable NIO. To do this, perform the following steps on each of the Oracle Virtual Directory instances:

1. Stop Oracle Virtual Directory by typing:

    ```
    ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ovd1
    ```

2. Edit the file:

    ```
    ORACLE_INSTANCE/config/OVD/component/listener.os_xml
    ```

    Locate the section for LDAP SSL listener, which looks like this:

    ```
    <ldap version="20" id="LDAP SSL Endpoint">
    <port>7501</port>
    <host>0.0.0.0</host>
    .........
    .........
    <tcpNoDelay>true</tcpNoDelay>
    <readTimeout>180000</readTimeout>
    </socketOptions>
    </ldap>
    ```

    Modify this section so that it looks like this:

    ```
    <ldap version="20" id="LDAP SSL Endpoint">
    <port>7501</port>
    <host>0.0.0.0</host>
    .........
    .........
    <tcpNoDelay>true</tcpNoDelay>
    <readTimeout>180000</readTimeout>
    </socketOptions>
    <useNIO>false</useNIO>
    ```

```
</ldap>
```

3. Save the file.

4. Restart Oracle Virtual Directory using the command:

   ```
   ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ovd1
   ```

5. Repeat for each Oracle Virtual Directory instance.

9.6 Validating the Oracle Virtual Directory Instances

To validate the Oracle Virtual Directory instances, ensure that you can connect to each Oracle Virtual Directory instance and the load balancing router using these `ldapbind` commands.

Follow the steps in Section 9.4.2.2, "Configuring Oracle Virtual Directory for SSL" before running the `ldapbind` command with the SSL port.

```
ldapbind -h ovdhost1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h idstore.mycompany.com -p 389 -D "cn=orcladmin" -q

ldapbind -h ovdhost1.us.oracle.com -p 7501 -D "cn=orcladmin" -q -U 1
ldapbind -h ovdhost2.us.oracle.com -p 7501 -D "cn=orcladmin" -q -U 1
```

9.7 Creating ODSM Connections to Oracle Virtual Directory

Before you can manage Oracle Virtual Directory you must create connections from ODSM to each of your Oracle Virtual Directory instances. To do this, proceed as follows:

1. Access ODSM through the load balancer address:
   `http://admin.mycompany.com/odsm`

2. Validate that Oracle Directory Services Manager can create connections to Oracle Internet Directory and Oracle Virtual Directory. Follow these steps to create connections to Oracle Internet Directory and Oracle Virtual Directory:

   To create connections to Oracle Internet Directory, follow these steps:

   a. Launch Oracle Directory Services Manager:

      `http://admin.mycompany.com/odsm`

   b. Create a connection to the Oracle Internet Directory virtual host by providing the following information in ODSM:

      Host: `policystore.mycompany.com`

      Port: `636`

      Enable the SSL option

      User: `cn=orcladmin`

      Password: `ldap-password`

   To create connections to Oracle Virtual Directory, follow these steps. Create connections to each Oracle Virtual Directory node separately. Using the Oracle Virtual Directory load balancer virtual host from ODSM is not supported:

   a. Launch Oracle Directory Services Manager:

```
http://admin.mycompany.com/odsm/
```

b. Create a direct connection to Oracle Virtual Directory on OVDHOST1 providing the following information in ODSM:

```
Host: ovdhost1.mycompany.com
Port: 8899  (The Oracle Virtual Directory proxy port)
Enable the SSL option
User: cn=orcladmin
Password: password_to_connect_to_OVD
```

9.8 Creating Adapters in Oracle Virtual Directory

Oracle Virtual Directory communicates with other directories through adapters.

Before you can start using Oracle Virtual Directory as an Identity Store, you must create adapters to each of the directories you want to use.The procedure is slightly different, depending on the directory you are connecting to. The following sections show how to create adapters for three directories:

- Section 9.8.1, "Creating Adapters for Oracle Internet Directory"
- Section 9.8.2, "Creating Adapters for Microsoft Active Directory Server"

9.8.1 Creating Adapters for Oracle Internet Directory

Oracle Virtual Directory is not required when you use Oracle Internet Directory as the back-end directory. However, if you want to access your Oracle Internet Directory through Oracle Virtual Directory, create the following Oracle Virtual Directory adapters.

User Adapter

Create the user adapter on the Oracle Virtual Directory instances running on OVDHOST1 and OVDHOST2 individually. Follow these steps to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at: `http://admin.mycompany.com/odsm`.

2. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

3. On the Home page, click the **Adapter** tab.

4. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.

5. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	**Adapter Type**	LDAP
	Adapter Name	User Adapter
	Adapter Template	User_OID
Connection	**Use DNS for Auto Discovery**	No

Screen	Field	Value/Step
	Host	idstore.mycompany.com
	Port	389
	Server Proxy Bind DN	cn=orcladmin
	Proxy Password	Password for orcladmin user.
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	dc=mycompany,dc=com
	Mapped Namespace[1]	dc=mycompany,dc=com

[1] The Remote Base is the context in Oracle Virtual Directory where your information is stored. The Mapped Namespace is the context in Oracle Internet Directory where your information is stored. These are usually the same, but need not be.

Verify that the summary is correct and then click **Finish**.

6. Edit the User Adapter as follows:

   a. Select the User Adapter.

   b. Click the **Plug-ins** tab.

   c. Click the **User Management** Plug-in in the plug-ins table, then click **Edit**. The plug-in editing window appears.

   d. In the Parameters table, update the parameter values as follows:

Parameter	Value	Default
directoryType	oid	Yes
pwdMaxFailure	10	Yes
oamEnabled	true[1]	
mapObjectclass	container=orclContainer	Yes

[1] Set oamEnabled to true only if you are using Oracle Access Manager.

   e. Click **OK**.

   f. Click **Apply**.

Change Log Adapter

To use the changelog adapter, you must first enable changelog on the connected directory. To test whether the directory is changelog enabled, type:

```
ldapsearch -h directory_host -p ldap_port -D bind_dn -w password -b '' -s base
'objectclass=*' lastchangenumber
```

The change log adapter is only required if you are implementing Oracle Identity Manager.

Create the change log adapter on the Oracle Virtual Directory instances running on OVDHOST1 and OVDHOST2 individually. Follow these steps to create the Change Log Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at: `http://admin.mycompany.com/odsm`.

2. Create connections to each of the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2`, if they do not already exist.

3. Connect to an Oracle Virtual Directory instance by using the appropriate connection entry.

4. On the Home page, click the **Adapter** tab.

5. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.

6. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	**Adapter Type**	LDAP
	Adapter Name	Change Log Adapter
	Adapter Template	`Changelog_OID`
Connection	**Use DNS for Auto Discovery**	No
	Host	`idstore.mycompany.com`
	Port	`389`
	Server Proxy Bind DN	`cn=orcladmin`
	Proxy Password	Password for `orcladmin` user.
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	(Do not assign.)
	Mapped Namespace	`cn=changelog`
Summary		Verify that the summary is correct, then click **Finish**.

7. To edit the change adapter follow these steps.

   a. Select the Change Log Adapter.

   b. Click the **Plug-ins** tab.

   c. In the Deployed Plug-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

   d. In the Parameters table, update the parameter values.

   Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the `modifierDNFilter`, `sizeLimit`, and `targetDNFilter` properties to the adapter.

Parameter	Value	Comments
directoryType	`oid`	Default

Parameter	Value	Comments
mapAttribute	targetGUID=orclguid	Default
requiredAttribute	orclGUID	Default
modifierDNFilter	!(modifiersname=cn=orcladmin)	Create
sizeLimit	1000	Create
targetDNFilter	dc=mycompany,dc=com	Create
	Search base from which reconciliation must happen. This value must be the same as the LDAP SearchDN that is specified during Oracle Identity Manager installation.	
mapUserState	true	Update
oamEnabled	true[1]	Update

[1] Set oamEnabled to true only if you are using Oracle Access Manager.

    e. Click **OK**.

    f. Click **Apply**.

9.8.2 Creating Adapters for Microsoft Active Directory Server

User Adapter

Create the user adapter on the Oracle Virtual Directory instances running on OVDHOST1 and OVDHOST2 individually. Follow these steps to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Start the Administration Server and the WLS_ODSM Managed Servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. In a web browser, go to Oracle Directory Services Manager (ODSM) at: http://admin.mycompany.com/odsm.

3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

4. On the Home page, click the **Adapter** tab.

5. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.

6. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	**Adapter Type**	LDAP
	Adapter Name	User Adapter
	Adapter Template	User_ActiveDirectory
Connection	**Use DNS for Auto Discovery**	No
	Host	Active Directory host/virtual name

Screen	Field	Value/Step
	Port	Active Directory SSL port
	Server Proxy Bind DN	The bind DN of a user who has access to Active Directory.
	Proxy Password	Password for the Active Directory administrative user.
	User SSL/TLS	Selected
	SSL Authentication Mode	Server Only Authentication
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	`dc=mycompany,dc=com`
	Mapped Namespace	`dc=mycompany,dc=com`

Verify that the summary is correct and then click **Finish**.

7. Edit the User Adapter as follows:

   a. Select the OIM User Adapter.

   b. Click the **Plug-ins** tab.

   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

   d. In the Parameters table, update the parameter values as follows:

Parameter	Value	Default
directoryType	`activedirectory`	Yes
exclusionMapping	`orclappiduser,uid=samaccountname`	
mapAttribute	`orclguid=objectGuid`	
mapAttribute	`uniquemember=member`	
addAttribute	`user,samaccountname=%uid%,%orclshortuid%`	
mapAttribute	`mail=userPrincipalName`	
mapAttribute	`ntgrouptype=grouptype`	
mapObjectclass	`groupofUniqueNames=group`	
mapObjectclass	`orclidxperson=user`	
pwdMaxFailure	10	Yes
oamEnabled	`True`[1]	
mapObjectClass	`inetorgperson=user`	Yes
mapPassword	`True`	Yes

[1] Set oamEnabled to true only if you are using Oracle Access Manager.

> **Note:** For language support, you must edit the User Management plug-in to add a new configuration parameter `oimLanguages`.
>
> For example, if the Managed Localization for the DisplayName while creating the user in Oracle Identity Manager is selected as French, then the value for `oimLanguages` in the User Management adapter plug-in should be `fr`. If you have other languages to be supported, say Japanese, then the value for the parameter should be `fr,ja`.
>
> The User Management plug-in has the following configuration parameter:
>
> `oimLanguages`: a comma-delimited list of language codes to be used in attribute language subtypes.
>
> This parameter is functional only when the `directoryType` parameter is set to `activedirectory`.

   e. Click **OK**.

   f. Click **Apply**.

Change Log Adapter

The change log adapter is only required if you are implementing Oracle Identity Manager.

Create the change log adapter on the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2` individually. Follow these steps to create the Change Log Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at: `http://admin.mycompany.com/odsm`.

2. Create connections to each of the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2`, if they do not already exist.

3. Connect to an Oracle Virtual Directory instance by using the appropriate connection entry.

4. On the Home page, click the **Adapter** tab.

5. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.

6. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	**Adapter Type**	LDAP
	Adapter Name	OIM Change Log Adapter
	Adapter Template	`Changelog_ ActiveDirectory`
Connection	**Use DNS for Auto Discovery**	No
	Host	Active Directory host/virtual name

Screen	Field	Value/Step
	Port	389
	Server Proxy Bind DN	The bind DN of a user who has access to Active Directory.
	Proxy Password	Password for oimadmin user.
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	(Do not assign.)
	Mapped Namespace	cn=changelog
Summary		Verify that the summary is correct, then click **Finish**.

7. To edit the change adapter follow these steps.

    a. Select the OIM Change Log Adapter.

    b. Click the **Plug-ins** tab.

    c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click "**Edit** in the plug-ins table. The plug-in editing window appears.

    d. In the Parameters table, update the parameter values.

    Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the, sizeLimit, and targetDNFilter properties to the adapter.

Parameter	Value	Comments
directoryType	activedirectory	Default
mapAttribute	targetGUID=objectGUID	Default
requiredAttribute	samaccountname	Default
sizeLimit	1000	Create
targetDNFilter	dc=mycompany,dc=com	Create
	Search base from which reconciliation must happen. This value must be the same as the LDAP SearchDN that is specified during Oracle Identity Manager installation.	
mapUserState	true	Update
oamEnabled	true[1]	
virtualDITAdapter Name	The name of the User adapter's name	Create

[1] Set oamEnabled to true only if you are using Oracle Access Manager.

> **Note:** **virtualDITAdapterName** identifies the corresponding user
> profile adapter name. For example, in a single-directory deployment,
> you can set this parameter value to `User Adapter`, which is the user
> adapter name. In a split-user profile scenario, you can set this
> parameter to `J1;A2`, where `J1` is the JoinView adapter name, and `A2`
> is the corresponding user adapter in the `J1`.

    e. Click **OK**.

    f. Click **Apply**.

9.9 Tuning Oracle Virtual Directory

After installing Oracle Virtual Directory, you must tune it as described in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

In particular, set the following attribute values when deploying Oracle Identity Management for Fusion Applications:

Attribute	Value
timeout	60000
maxPoolSize	20

9.10 Backing Up the Oracle Virtual Directory Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install 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. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the directory tier:

    a. Shut down the instance using opmnctl located under the *ORACLE_INSTANCE*/bin directory:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

    b. Create a backup of the Middleware home on the directory tier. On Linux, as the `root` user, type:

```
tar -cvpf BACKUP_LOCATION/dirtier.tar MW_HOME
```

    c. Create a backup of the Instance home on the directory tier as the `root` user:

```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```

d. Start up the instance using `opmnctl` located under the *ORACLE_ INSTANCE*/`bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager.

3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the *ORACLE_ BASE*/`admin/domainName/aserver directory`. On Linux, type:

```
IDMHOST1> tar cvf edgdomainback.tar ORACLE_BASE/admin/domainName/aserver
```

Note: Create backups on all machines in the directory tier by following the steps shown in this section.

For more information about backing up the directory tier configuration, see Section 19.4, "Performing Backups and Recoveries."

10

Preparing Directories Other than Oracle Internet Directory

This chapter explains how to prepare directories other than Oracle Internet Directory for Oracle Access Manager and Oracle Identity Manager. This requires the directory schema to be extended for supporting Oracle Access Manager-specific schema elements.

Deployments that allow schema extensions in the back-end directory use the approach explained in Section 10.1, "Preparing a Directory for Fusion Applications, Oracle Access Manager, and Oracle Identity Manager."

In deployments where the back-end schema extension is not allowed in the enterprise Identity Store, use Oracle Internet Directory as a shadow directory and use Oracle Virtual Directory to merge the entities from the directories. The configuration requirements for such deployments is described in Section 10.2, "Configuring Multiple Directories as an Identity Store: Split Profile with Oracle Virtual Directory."

Some deployments might have both internal and external entities. Configuration requirements for such deployments is described in Section 10.3, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories."

This chapter contains the following topics:

- Section 10.1, "Preparing a Directory for Fusion Applications, Oracle Access Manager, and Oracle Identity Manager"

- Section 10.2, "Configuring Multiple Directories as an Identity Store: Split Profile with Oracle Virtual Directory"

- Section 10.3, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories"

10.1 Preparing a Directory for Fusion Applications, Oracle Access Manager, and Oracle Identity Manager

This section explains how to configure Active Directory.

It contains the following topics:

- Section 10.1.1, "Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Management"

- Section 10.1.2, "Disable Oracle Virtual Directory Access Control"

10.1.1 Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Management

This section describes how to configure Active Directory. Extend the schema in Active Directory as follows.

1. Locate the following files:

   IDM_ORACLE_HOME/oam/server/oim-intg/ldif/ad/schema/ADUserSchema.ldif

   IDM_ORACLE_HOME/oam/server/oim-intg/ldif/ad/schema/AD_oam_pwd_schema_add.ldif

2. In both these files, replace the `domain-dn` with the appropriate `domain-dn` value

3. Use `ldapadd` from the command line to load the two LDIF files, as follows.

   ```
   ldapadd -h activedirectoryhostname -p activedirectoryportnumber -D AD_
   administrator -q -c -f file
   ```

   where `AD_administrator` is a user which has schema extension privileges to the directory

   For example:

   ```
   ldapadd -h "activedirectoryhost.mycompany.com" -p 389 -D adminuser -q -c -f
   ADUserSchema.ldif
   ldapadd -h "activedirectoryhost.mycompany.com" -p 389 -D adminuser -q -c -f AD_
   oam_pwd_schema_add.ldi
   ```

4. Then go to:

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

   Run the following command to extend Active Directory schema:

   ```
   sh extendadschema.sh -h AD_host -p AD_port -D 'administrator@mydomain.com' -AD
   "dc=mydomain,dc=com" -OAM true
   ```

   The command is `extendadschema.bat` on Windows.

10.1.2 Disable Oracle Virtual Directory Access Control

f you are using Active Directory as your directory store you need to Disable the Access Control Flag in OVD. To do this perform the following steps:

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:
   `http://admin.mycompany.com/odsm`

2. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

3. Navigate to **Advanced->ServerSettings->Settings**.

4. Deselect **Enable Access Control**.

5. Click **Save**.

6. Click **Apply**.

10.2 Configuring Multiple Directories as an Identity Store: Split Profile with Oracle Virtual Directory

This section describes how to configure two parallel directories. Oracle Virtual Directory links them together to present a single DIT view to clients. It contains the following topics:

- Section 10.2.1, "Directory Structure Overview"
- Section 10.2.2, "Configuring Oracle Virtual Directory Adapters and Plug-ins"

10.2.1 Directory Structure Overview

Figure 10–1 shows the directory structure in the primary store and application store.

Figure 10–1   Directory Structure

Figure 10–2 shows how the DIT appears to a user or client application.

Figure 10–2   Client View of the DIT
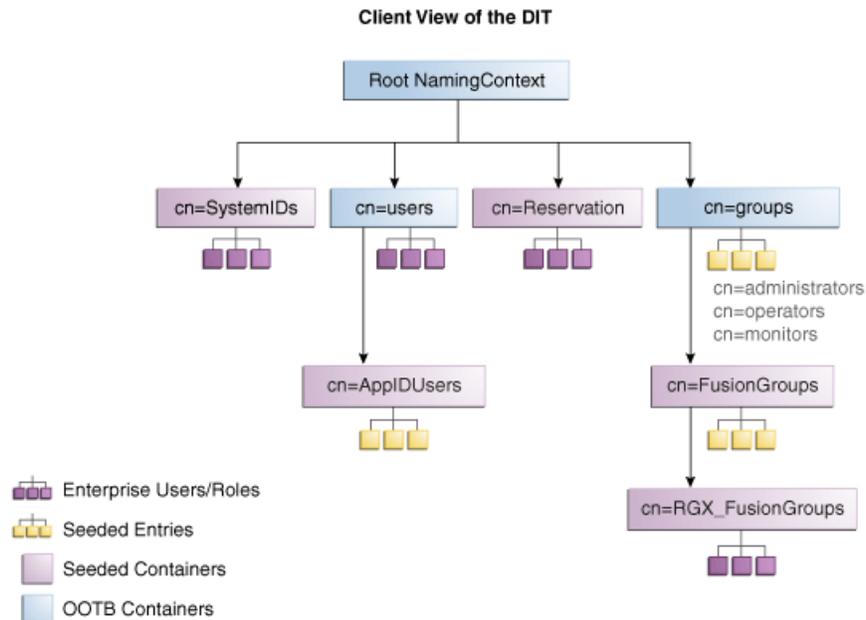
10.2.2 Configuring Oracle Virtual Directory Adapters and Plug-ins

Figure 10–3 provides an overview of the configuration.

Figure 10–3   Configuration Overview

Create the user adapter on the Oracle Virtual Directory instances running on
OVDHOST1 and OVDHOST2 individually. Follow these steps to create the User Adapter
in Oracle Virtual Directory using Oracle Directory Services Manager:

1. Start the Administration Server and the WLS_ODSM Managed Servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

3. Create connections to each of the Oracle Virtual Directory instances running on OVDHOST1 and OVDHOST2, if they do not already exist.

4. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

5. On the Home page, click the **Adapter** tab.

6. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.

7. Create new adapters using the New Adapter Wizard, with the parameters shown in the following tables.

10.2.2.1 User/Role Adapter A1

Table 10–1 User/Role Adapter A1

Screen	Field	Value
Type	Adapter Type	LDAP
	Name	User_Adapter_A1
	Adapter Template	FAPrimary_User_OID
		FAPrimary_User_ActiveDirectory
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: ad.mycompany.com
	Port	Enter the port to connect to the LDAP directory on.
	Use SSL/TLS	Select this value if you connect to your LDAP directory using SSL or if you are using Active Directory.
	SSL Authentication Mode	If you connect to your LDAP directory using SSL, choose the authentication mode. If using Active Directory select Server Only Authentication (Mutual Authentication).
	Server Proxy Bind DN	A bind DN that has administrative rights on the directory server. For example: cn=AdminUser,cn=system,dc=mycompany,dc=com
	Proxy Password	Password for Server Proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	dc=mycompany, dc=com
	Mapped Namespace[1]	dc=mycompany, dc=com

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

10.2.2.2 User/Role Adapter A2

Table 10–2 User/Role Adapter A2

Screen	Field	Value
Type	Adapter Type	`LDAP`
	Name	`User_Adapter_A2`
	Adapter Template	`FAJoiner_User_OID`
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: `ldap.mycompany.com`
	Port	Enter the port to connect to the LDAP directory on.
	Use SSL/TLS	Select this value if you connect to your LDAP directory using SSL or if you are using Active Directory.
	SSL Authentication Mode	If you connect to your LDAP directory using SSL, choose the Authentication mode.
	Server Proxy Bind DN	A bind DN that has administrative rights on the directory server. For example: `cn=AdminUser,cn=system,dc=mycompany,dc=com`
	Proxy Password	Password for Server Proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	`dc=mycompany, dc=com`
	Mapped Namespace[1]	`dc=mycompany, dc=com`

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle virtual directory. If this is not the case, then modify accordingly.

10.2.2.3 User/Role Adapter A3

Table 10–3 User/Role Adapter A3

Screen	Field	Value
Type	Adapter Type	`LDAP`
	Name	`User_Adapter_A3`
	Adapter Template	`User_OID`
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No

Table 10–3 (Cont.) User/Role Adapter A3

Screen	Field	Value
	Host	Enter the Host or Virtual Name of the directory host, for example: ad.mycompany.com
	Port	Enter the Port to connect to the LDAP directory on.
	Use SSL/TLS	Select this value if you connect to your LDAP directory using SSL or if you are using Active Directory.
	SSL Authentication Mode	If you connect to your LDAP directory using SSL, choose the Authentication mode. If using Active Directory select Server Only Authentication (Mutual Authentication).
	Server Proxy Bind DN	A bind DN that has administrative rights on the directory server. For example: cn=AdminUser,cn=system,dc=mycompany,dc=com
	Proxy Password	Password for Server Proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	dc=mycompany, dc=com
	Mapped Namespace[1]	dc=mycompany, dc=com

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle virtual directory. If this is not the case, then modify accordingly.

10.2.2.4 User/Role Adapter J1 (JoinView Adapter)

Table 10–4 User/Role Adapter J1 (JoinView Adapter)

Screen	Field	Value
Type	Adapter Type	Join
	Name	Join_Adapter_J1
	Adapter Template	Default
Settings	Adapter	dc=mycompany, dc=com
	Primary Adapter	User_Adapter_A1
	Bind Adapters	User_Adapter_A1

After creating the JoinView adapter, perform the following steps:

1. Click **Join_Adapter_J1** from the **Adapters** list and click the **Edit** button.

2. In the Join Rules box click **Add new Join Rule**.

3. Enter the following information:

   - **Joined Adapter**: User_Adapter_A2

   - **Type**: com.octetstring.vde.join.shadowJoiner

   - **Condition**:cn

4. Click **OK** to save the condition.

5. Click **Apply**.

10.2.2.5 Changelog Adapter C1

Table 10–5   Changelog Adapter C1

Screen	Field	Value
Type	Adapter Type	`LDAP`
	Name	`Changelog_Adapter_C1`
	Adapter Template	`Changelog_OID`
		`Changelog_ActiveDirectory`
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: `ad.mycompany.com`
	Port	Enter the port to connect to the LDAP directory on.
	Proxy Password	Password for Server Proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	
	Mapped Namespace[1]	`cn=changelog`

[1]   Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle virtual directory. If this is not the case, then modify accordingly.

To edit the Change Log Adapter C1, follow these steps:

1. Select **Changelog_Adapter_C1**.

2. Click the **Plug-ins** tab.

3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

4. In the **Parameters** table, update the parameter values.Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the modifierDNFilter, sizeLimit, and targetDNFilter properties to the adapter.

Table 10–6   Values in Parameters Table

Parameter	Value	Comments

modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format:
	
	`"!(modifiersname=cn=BindDN)"`
	
	For example:
	
	`"!(modifiersname=cn=orclAdminUser,cn=s ystemids,dc=mycompany,dc=com)"`
		Create

sizeLimit	1000	Create
targetDNFilter	`dc=mycompany,dc=com`	Create

Table 10–6   (Cont.) Values in Parameters Table

Parameter	Value	Comments
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	Join_Adapter_J1;User_Adapter_A1	Create

10.2.2.6 Changelog Adapter C2

Table 10–7   Changelog Adapter C2

Screen	Field	Value
Type	Adapter Type	`LDAP`
	Name	`Changelog_Adapter_C2`
	Adapter Template	`Changelog_OID`
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: `ad.mycompany.com`
	Port	Enter the port to connect to the LDAP directory on.
	Proxy Password	Password for server proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	
	Mapped Namespace[1]	`cn=changelog`

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

To edit the Change Log Adapter C2, follow these steps:

1. Select **Changelog_Adapter_C2**.

2. Click the **Plug-ins** tab.

3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

4. In the **Parameters** table, update the parameter values.Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the modifierDNFilter, sizeLimit, and targetDNFilter properties to the adapter.

Table 10–8   Values in Parameters Table

Parameter	Value	Comments

modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format:
	
	 `"!(modifiersname=cn=BindDN)"`
	
	 For example:
	
	 `"!(modifiersname=cn=orclAdminUser,cn=s`
	`ystemids,dc=mycompany,dc=com)"`
		Create

sizeLimit	1000	Create
targetDNFilter	`dc=mycompany,dc=com`	Create
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	Join_Adapter_J1;User_Adapter_A2	Create
virtualDITAdapterName	User_Adapter_A3	Create

10.2.2.7 Creating Oracle Virtual Directory Global Plug-ins

To create a Global Oracle Virtual Directory plug-in

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

2. Create connections to each of the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2`, if they do not already exist.

3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

4. On the Home page, click the **Adapter** tab.

5. Click the **+** next to **Global Plugins** in the left pane.

6. Click **Create Plugin**.

7. Create the Global Consolidated Changelog Plug-in and the Global FAUserRole Plugin as follows:

Global Consolidated Changelog Plug-in

Enter the following values to create the Global Consolidated Plug-in:

Name: `Global Consolidated Changelog`

Class: Click **Select** then choose: **ConsolidatedChangelog**

Click **OK** when finished.

Global FAUserRole Plugin

Enter the following values to create the Global Consolidated Plug-in:

Name: `FA User Role Plugin`

Class: Click **Select** then choose: **FAUserRolePlugIn**

Click **Create Parameter**

Create the following parameters:

Table 10–9   Parameters for FAUserRole Plugin

Name	Value
objectWrite	`objectclass=orclAppIDUser;User_Adapter_A3`
objectWrite	`objectclass=orclAppIDGroup;User_Adapter_A3`
objectWrite	`objectclass=orclIDXGroup;User_Adapter_A1; User_Adapter_A3`
objectWrite	`objectclass=container;User_Adapter_A3`

Click **OK** when finished.

10.3 Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories

In this configuration, all the Oracle specific attributes and Oracle specific entities are created in the Policy Store (OID) directory. Enterprise Identity Store is an LDAP directory.

> **Note:**   The Oracle Internet Directory that is to be used is not necessarily the PolicyStore Oracle Internet Directory. Conceptually, a non-AD directory can be used as the second directory. For convenience, Policy Store Oracle Internet Directory is referred to here.

The following conditions are assumed:

- Enterprise Directory Identity data is in one or more directories. Application-specific attributes on the user / group are stored in the Enterprise Directory.

- Application-specific entries are in Application Directory. (AppIDs and Enterprise Roles are stored in Application Directory)

This section contains the following topics:

- Section 10.3.1, "Topology"

- Section 10.3.2, "Directory Structure Overview"

- Section 10.3.3, "Configuring Oracle Virtual Directory Adapters and Plug-ins"

10.3.1 Topology

Figure 10–4 is an overview of the topology:

Figure 10–4   Overview of Topology
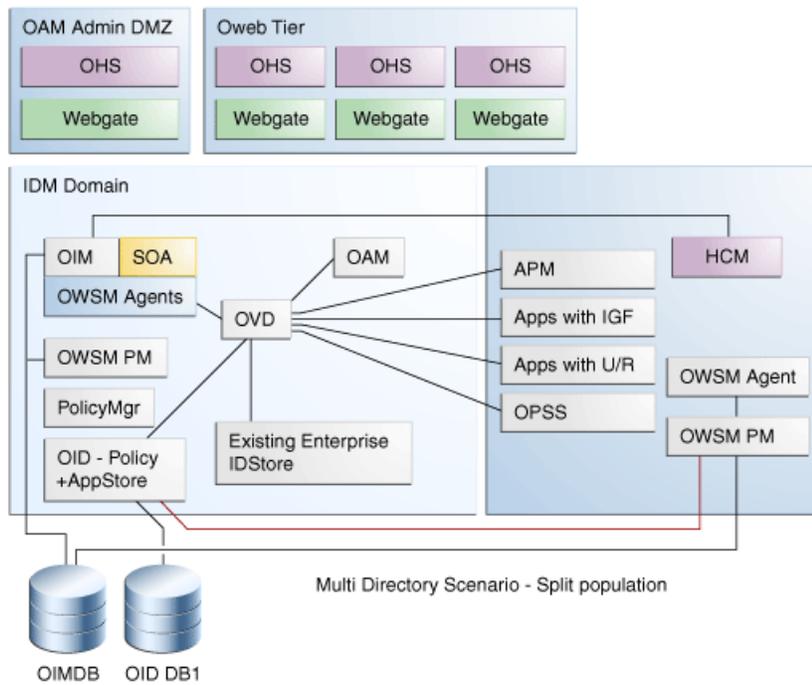
10.3.2 Directory Structure Overview

Figure 10–5 shows the directory structure in the internal and external directories.

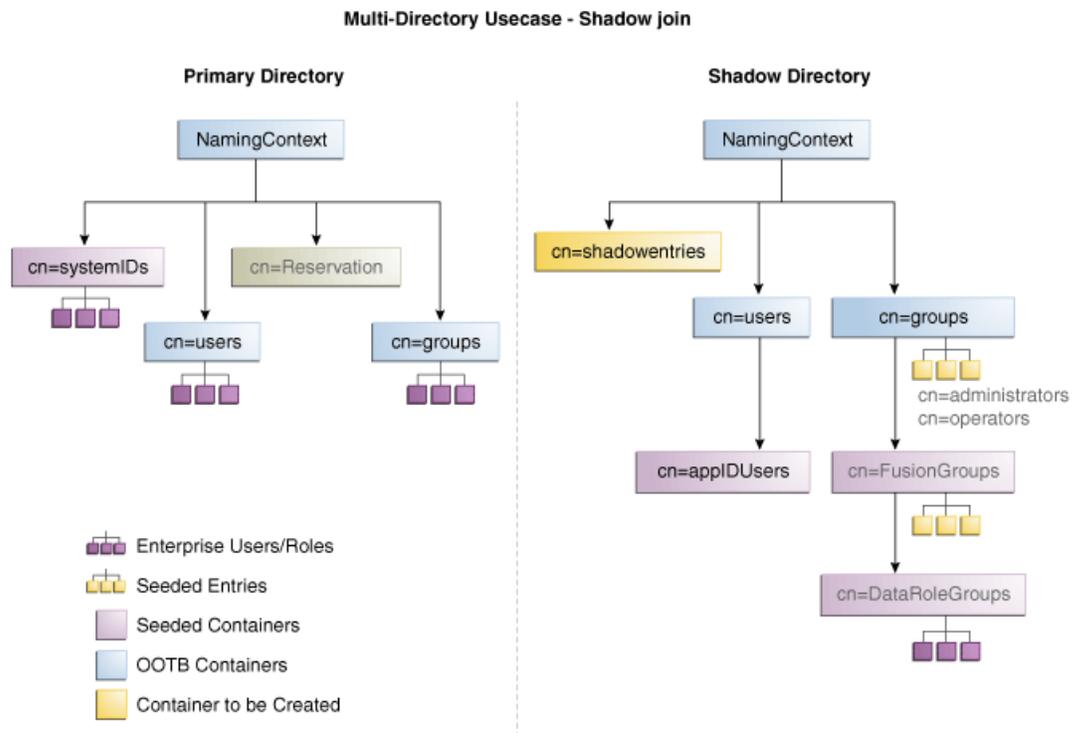**Figure 10–5   Directory Structure**

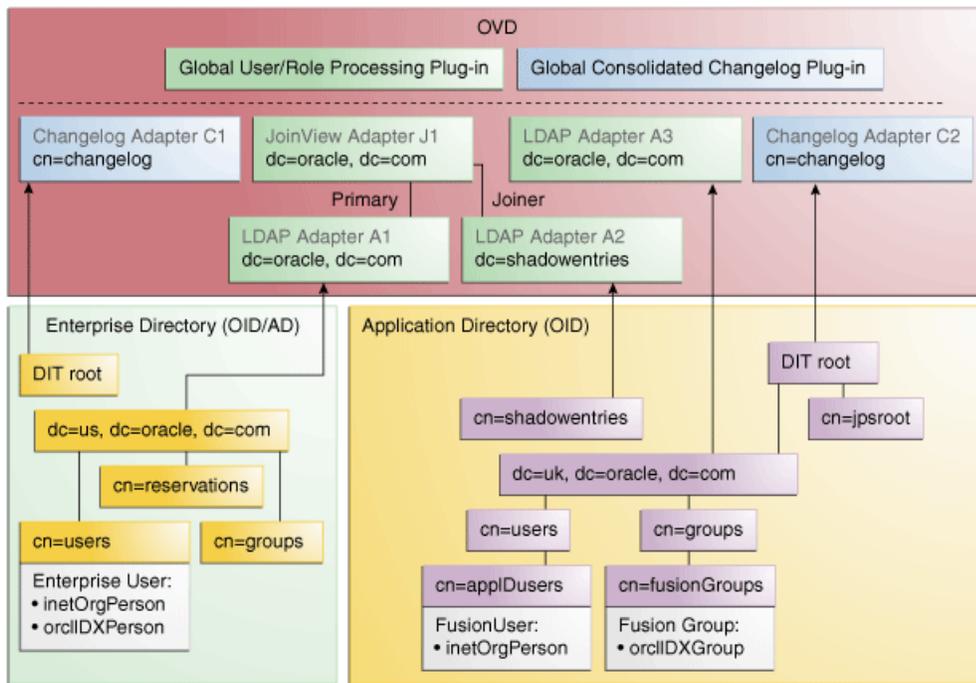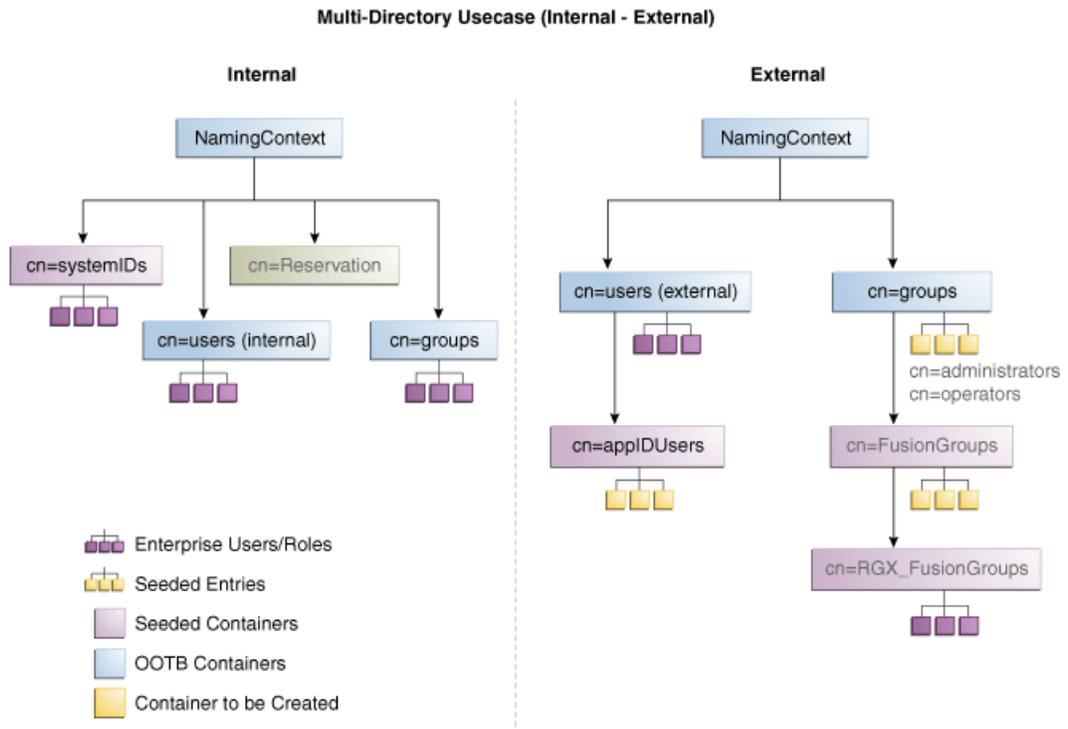Figure 10–6 shows how the DIT appears to a user or client application.

Figure 10–6   Client View of the DIT
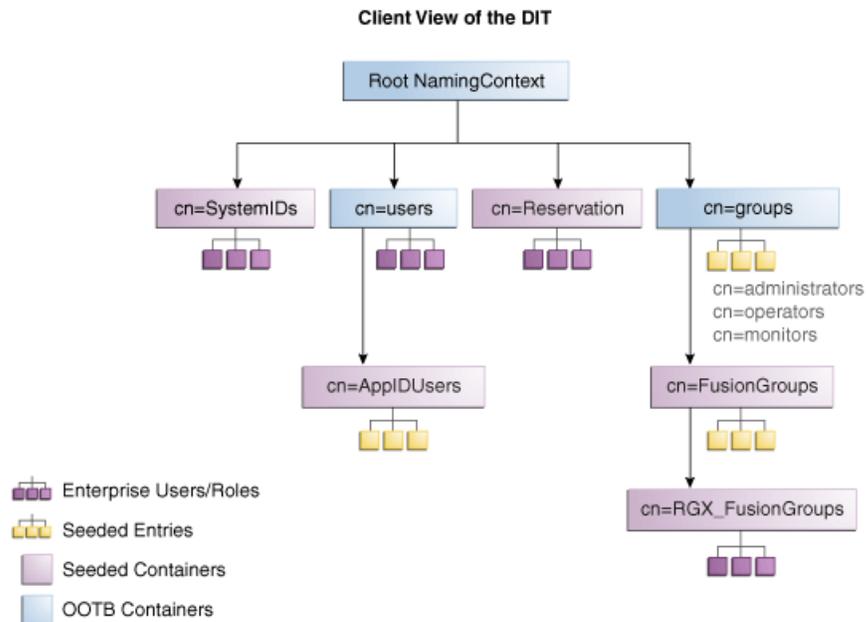
10.3.3 Configuring Oracle Virtual Directory Adapters and Plug-ins

Figure 10–7 provides an overview of the configuration.

Figure 10–7   Configuration Overview
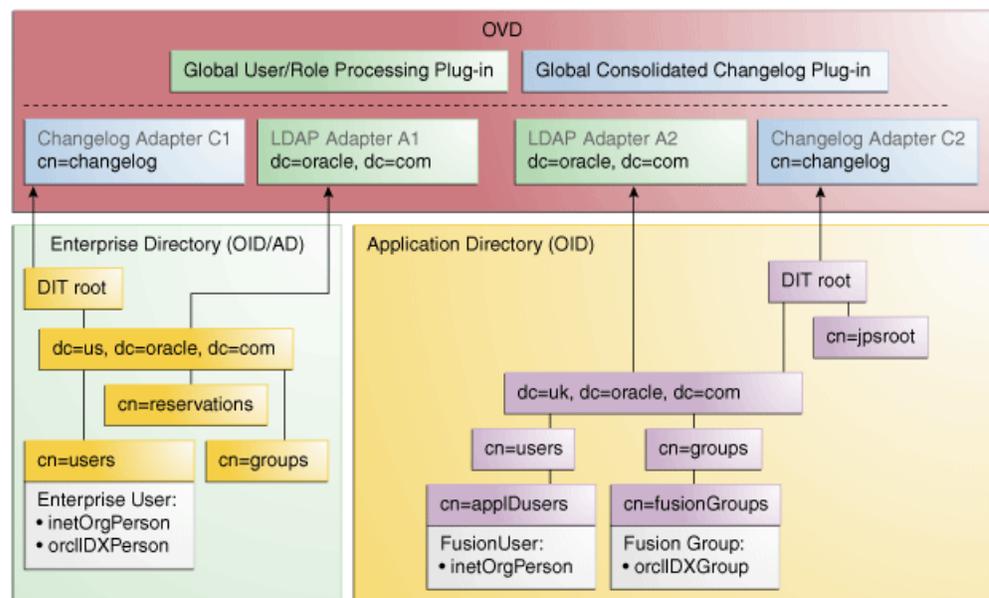
Create the user adapter on the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2` individually. Follow these steps to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager:

1. If they are not already running, start the Administration Server and the WLS_
   ODSM Managed Servers as described in Section 19.1, "Starting and Stopping
   Oracle Identity Management Components."

2. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

3. Create connections to each of the Oracle Virtual Directory instances running on
   `OVDHOST1` and `OVDHOST2`, if they do not already exist.

4. Connect to each Oracle Virtual Directory instance by using the appropriate
   connection entry.

5. On the Home page, click the **Adapter** tab.

6. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the
   adapter window.

7. Create new adapters using the New Adapter Wizard, with the parameters shown
   in the following tables.

10.3.3.1 User/Role Adapter A1

Table 10–10   User/Role Adapter A1

Screen	Field	Value
Type	Adapter Type	LDAP
	Name	User_Adapter_A1
	Adapter Template	User_OID
		User_ActiveDirectory
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: ad.mycompany.com
	Port	Enter the port to connect to the LDAP directory on.
	Use SSL/TLS	Select this value if you connect to your LDAP directory using SSL or if you are using Active Directory.
	SSL Authentication Mode	If you connect to your LDAP directory using SSL, choose the authentication mode. If using Active Directory select Server Only Authentication (Mutual Authentication).
	Server Proxy Bind DN	The DN of a user that Oracle Virtual Directory can use to connect to AD and perform any operations. A user called oimAdminUser is created in the section Section 11.4, "Preparing the Identity Store" which can be used for this purpose.
	Proxy Password	Password for Server Proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	dc=mycompany, dc=com
	Mapped Namespace[1]	dc=mycompany, dc=com

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

10.3.3.2 User/Role Adapter A2

Table 10–11   User/Role Adapter A2

Screen	Field	Value
Type	Adapter Type	LDAP
	Name	User_Adapter_A2
	Adapter Template	User_OID
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: ldap.mycompany.com
	Port	Enter the port to connect to the LDAP directory on.
	Use SSL/TLS	Select this value if you connect to your LDAP directory using SSL or if you are using Active Directory.
	SSL Authentication Mode	If you connect to your LDAP directory using SSL, choose the authentication mode. If you are using Active Directory, choose **Server Only Authentication/Mutual Authentication**.
	Server Proxy Bind DN	The DN of a user that Oracle Virtual Directory can use to connect to AD and perform all operations. The user oimAdminUser, which is created in Section 11.4, "Preparing the Identity Store," can be used for this purpose.
	Proxy Password	Password for server proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	dc=mycompany, dc=com
	Mapped Namespace[1]	dc=mycompany, dc=com

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

10.3.3.3 Changelog Adapter C1

Table 10–12   Changelog Adapter C1

Screen	Field	Value
Type	Adapter Type	LDAP
	Name	Changelog_Adapter_C1
	Adapter Template	Changelog_OID
		Changelog_ActiveDirectory
		Choose the correct template for the LDAP directory you are connecting to.

Table 10–12 (Cont.) Changelog Adapter C1

Screen	Field	Value
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: `ad.mycompany.com`
	Port	Enter the port to connect to the LDAP directory on.
	Proxy Password	Password for server proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	
	Mapped Namespace[1]	`cn=changelog`

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

To edit the Change Log Adapter C1, follow these steps:

1. Select the OIM change log adapter **Changelog_Adapter_C1**.

2. Click the **Plug-ins** tab.

3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

4. In the **Parameters** table, update the parameter values.Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the modifierDNFilter, sizeLimit, and targetDNFilter properties to the adapter.

Table 10–13 Values in Parameters Table

Parameter	Value	Comments

modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format:
	`"!(modifiersname=cn=BindDN)"`
	For example:
	`"!(modifiersname=cn=orclAdminUser,cn=systemids,dc=mycompany,dc=com)"`
		Create

sizeLimit	1000	Create
targetDNFilter	`dc=mycompany,dc=com`	Create
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	The adapter name of User/Role Adapter A1: `User_Adapter_A1`	Create

10.3.3.4 Changelog Adapter C2

Table 10–14   Changelog Adapter C2

Screen	Field	Value
Type	Adapter Type	`LDAP`
	Name	`Changelog_Adapter_C2`
	Adapter Template	`Changelog_OID`
		Choose the correct template for the LDAP directory you are connecting to.
Connection	Use DNS for Auto Discovery	No
	Host	Enter the host or virtual name of the directory host, for example: `ad.mycompany.com`
	Port	Enter the port to connect to the LDAP directory on.
	Proxy Password	Password for server proxy account
Connection Test		Validate that the test succeeds
Namespace	Remote Base	
	Mapped Namespace[1]	`cn=changelog`

[1] Mapped namespace is the location in the target directory. This example assumes that the target directory has the same structure that appears in Oracle Virtual Directory. If this is not the case, then modify accordingly.

To edit the Change Log Adapter C2, follow these steps:

1. Select the OIM change log adapter **Changelog_Adapter_C2**.

2. Click the **Plug-ins** tab.

3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.

4. In the **Parameters** table, update the parameter values.Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the modifierDNFilter, sizeLimit, and targetDNFilter properties to the adapter.

Table 10–15   Values in Parameters Table

Parameter	Value	Comments

modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format:
	
	`"!(modifiersname=cn=`*BindDN*`)"`
	
	For example:
	
	`"!(modifiersname=cn=orclAdminUser,cn=systemids,dc=mycompany,dc=com)"`
		Create

sizeLimit	1000	Create
targetDNFilter	`dc=mycompany,dc=com`	Create
mapUserState	true	Update
oamEnabled	true	Update

Table 10–15   (Cont.) Values in Parameters Table

Parameter	Value	Comments
virtualDITAdapterName	The adapter name of User/Role adapter A2: `User_Adapter_A2`	Create

10.3.3.5 Creating Oracle Virtual Directory Global Plug-ins

To create a Global Oracle Virtual Directory plug-in

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

2. Create connections to each of the Oracle Virtual Directory instances running on `OVDHOST1` and `OVDHOST2`, if they do not already exist.

3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

4. On the Home page, click the **Adapter** tab.

5. Click the **+** next to **Global Plugins** in the left pane.

6. Click **Create Plugin**.

7. Create the Global Consolidated Changelog Plug-in and the Global FAUserRole Plugin as follows:

Global Consolidated Changelog Plug-in

Enter the following values to create the Global Consolidated Plug-in:

Name: `Global Consolidated Changelog`

Class: Click **Select** then choose: **ConsolidatedChangelog**

Click **OK** when finished.

Global FAUserRole Plugin

Enter the following values to create the Global Consolidated Plug-in:

Name: `FA User Role Plugin`

Class: Click **Select** then choose: **FAUserRolePlugIn**

Click **Create Parameter**

Create the following parameters:

Table 10–16   Parameters for FAUserRole Plugin

Name	Value
objectWrite	`objectclass=orclAppIDUser;User_Adapter_A2`
objectWrite	`objectclass=orclAppIDGroup;User_Adapter_A2`
objectWrite	`objectclass=orclIDXGroup;User_Adapter_A1; User_Adapter_A2`
objectWrite	`objectclass=container;User_Adapter_A2`

Click **OK** when finished.

11

Preparing Identity and Policy Stores

This chapter describes how to prepare the Identity and Policy Stores. It contains the following sections:

- Section 11.1, "Backing up the LDAP Directories"
- Section 11.2, "Prerequisites"
- Section 11.3, "Preparing the Policy Store"
- Section 11.4, "Preparing the Identity Store"

11.1 Backing up the LDAP Directories

The procedures described in this chapter change the configuration of the LDAP directories that host the Identity and Policy Stores. Before performing any of these tasks, back up your LDAP directories. See Section 7.7, "Backing up the Oracle Internet Directory Configuration" and Section 9.10, "Backing Up the Oracle Virtual Directory Configuration" for more information.

11.2 Prerequisites

Before proceeding, ensure that the following statements are true:

- Oracle Identity Management 11*g* (11.1.1.5) is installed on `IDMHOST1`.
- Oracle Internet Directory is installed and configured (if required).
- Oracle Virtual Directory is installed and configured.
- Non-OID directories are installed and available (if required).

11.3 Preparing the Policy Store

This section describes how to prepare the Policy Store

It contains the following topics:

- Section 11.3.1, "Creating Policy Store Users and the Policy Container,"
- Section 11.3.2, "Reassociating the Policy and Credential Store,"

Before you can use the Policy Store, you must prepare it. This involves creating a JPS Root context in the Policy Store directory and reassociating the domain's internal Policy Store to use the external LDAP Policy Store.

11.3.1 Creating Policy Store Users and the Policy Container

Perform the following tasks on `IDMHOST1`:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME`, and `ORACLE_HOME`.

    Set `IDM_HOME` to `IDM_ORACLE_HOME`

    Set `ORACLE_HOME` to `IAM_ORACLE_HOME`

    Set `MW_HOME` to `/u01/app/oracle/product/fmw`.

    Set `JAVA_HOME` to `MW_HOME/jrockit-jdk1.6.0`.

2. Create a properties file, called `policystore.props` with the following contents:

    ```
    POLICYSTORE_HOST : policystore.mycompany.com
    POLICYSTORE_PORT : 389
    POLICYSTORE_BINDDN: cn=orcladmin
    POLICYSTORE_READONLYUSER: PolicyROUser
    POLICYSTORE_READWRITEUSER: PolicyRWUser
    POLICYSTORE_SEARCHBASE: dc=mycompany,dc=com
    POLICYSTORE_CONTAINER: cn=jpsroot
    ```

    Where:

    -   `POLICYSTORE_HOST` and `POLICYSTORE_PORT` are, respectively, the host and port of your Policy Store directory.

    -   `POLICYSTORE_BINDDN` Is an administrative user in the Policy Store directory

    -   `POLICYSTORE_READONLYUSER` and `POLICYSTORE_READWRITEUSER` are the names of Users you want to create in the Policy Store with Read Only and Read/Write privileges.

    -   `POLICYSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

    -   `POLCYSTORE_CONTAINER` is the name of the container used for OPSS policy information.

    In addition to creating the users, the command also creates the following groups:

    -   `OrclPolicyAndCredentialWritePrivilegeGroup`

    -   `OrclPolicyAndCredentialReadPrivilegeGroup`

    After creating the group, the tool adds the `readonlyuser` as a member of the `OrclPolicyAndCredentialReadPrivilegeGroup` and `readwriteuser` as a member of `OrclPolicyAndCredentialWritePrivilegeGroup`.

3. Configure the Policy Store using the command `idmConfigTool` which is located at:

    `IAM_ORACLE_HOME/idmtools/bin`

    > **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
    >
    > `IAM_ORACLE_HOME/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool.sh -configPolicyStore input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -configPolicyStore input_file=configfile
```

For example:

```
idmConfigTool.sh -configPolicyStore input_file=policystore.props
```

When the command runs you are prompted to enter the password of the account you are connecting to the Policy Store with. You are also asked to specify the passwords you want to assign to the accounts:

- POLICYSTORE_READONLYUSER

- POLICYSTORE_READWRITEUSER

Sample command output:

```
Enter Policy Store Bind DN password:
*** Creation of PolicyROUser ***
Apr 5, 2011 4:23:49 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_user.ldif
Enter User Password for PolicyROUser:
Confirm User Password for PolicyROUser:
*** Creation of PolicyRWUser ***
Apr 5, 2011 4:23:58 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_user.ldif
Enter User Password for PolicyRWUser:
Confirm User Password for PolicyRWUser:
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_group.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_
container.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_group_read_
member.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_group_
write_member.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_tuning.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oid_schemaadmin.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/policystore_user_
aci.ldif
The tool has completed its operation. Details have been logged to
/home/oracle/idmtools/automation.log
```

4. Check log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory from where you run the tool.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.3.2 Reassociating the Policy and Credential Store

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST `reassociateSecurityStore` command. Follow these steps:

1. From IDMHOST1, start the `wlst` shell from the *ORACLE_COMMON_HOME*/common/bin directory. For example, on Linux and UNIX-based systems, you would type:

   ```
   ./wlst.sh
   ```

   On Windows you would type:

   ```
   ./wlst.cmd
   ```

2. 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://ADMINVHN.mycompany.com:7001")
   ```

3. Run the `reassociateSecurityStore` command as follows:

   Syntax:

   ```
   reassociateSecurityStore(domain="domainName",admin="cn=orcladmin",
   password="orclPassword",ldapurl="ldap://LDAPHOST:LDAPPORT",servertype="OID",
   jpsroot="cn=jpsRootContainer")
   ```

   For example:

   ```
   wls:/IDMDomain/serverConfig> reassociateSecurityStore(domain="IDMDomain",
   admin="cn=orcladmin",password="password",
   ldapurl="ldap://policystore.mycompany.com:389",servertype="OID",
   jpsroot="cn=jpsroot")
   ```

   The output for the command is as follows:

   ```
   {servertype=OID, jpsroot=cn=jpsroot, admin=cn=orcladmin,
   domain=IDMDomain, ldapurl=ldap://policystore.mycompany.com:389,
   password=password}
   Location changed to domainRuntime tree. This is a read-only tree with
   DomainMBean as the root.
   For more help, use help(domainRuntime)

   Starting policy store reassociation.
   The store and ServiceConfigurator setup done.
   Schema is seeded into the store
   Data is migrated to the store
   Data in the store after migration has been tested to be available
   Update of in-memory jps configuration is done
   Policy store reassociation done.
   Starting credential store reassociation
   ```

```
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Credential store reassociation done
Starting Keystore reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Keystore reassociation done
Jps Configuration has been changed. Please restart the application server.
```

4. Restart the WebLogic Administration Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," after the command completes successfully.

11.4 Preparing the Identity Store

This section describes how to prepare the Identity Store. It contains the following topics:

- Section 11.4.1, "Extending Directory Schema for Oracle Access Manager"
- Section 11.4.2, "Creating Users and Groups for Oracle Access Manager"
- Section 11.4.3, "Creating Users and Groups for Oracle Identity Manager"
- Section 11.4.4, "Creating Users and Groups for Oracle WebLogic Server"
- Section 11.4.5, "Creating Users and Groups for Fusion Applications"
- Section 11.4.6, "Creating Access Control Lists in Non-Oracle Internet Directory Directories"
- Section 11.4.7, "Updating Oracle Virtual Directory Adapters"

11.4.1 Extending Directory Schema for Oracle Access Manager

Pre-configuring the Identity Store extends the schema in Oracle Internet Directory.

> **Note:** You do not need to preconfigure the Identity Store unless you are using Oracle Access Manager or Oracle Identity Manager.

To do this, perform the following tasks on IDMHOST1:

1. Set the environment variables: MW_HOME, JAVA_HOME, IDM_HOME and ORACLE_HOME.

   Set IDM_HOME to IDM_ORACLE_HOME

   Set ORACLE_HOME to IAM_ORACLE_HOME

2. Create a properties file, called extend.props with the following contents:

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
```

```
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
```

Where:

- `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory. If you are using a non-OID directory, then specify the Oracle Virtual Directory host (which should be `IDSTORE.mycompany.com`.)

- `IDSTORE_BINDDN` Is an administrative user in the Identity Store Directory

- `IDSTORE_USERSEARCHBASE` is the location in the directory where Users are Stored.

- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are Stored.

- `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

- `IDSTORE_SYSTEMIDBASE` is the location of a container in the directory where users can be placed when you do not want them in the main user container. This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.

3. Configure the Identity Store by using the command `idmConfigTool`, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

   > **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
   >
   > *IAM_ORACLE_HOME*/idmtools/bin

   The syntax of the command on Linux is:

   ```
   idmConfigTool.sh -preConfigIDStore input_file=configfile
   ```

   The syntax on Windows is:

   ```
   idmConfigTool.bat -preConfigIDStore input_file=configfile
   ```

   For example:

   ```
   idmConfigTool.sh -preConfigIDStore input_file=extend.props
   ```

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

   Sample command output:

   ```
   [orcl@rws3450009 dw_users]$
   /u01/app/oracle/product/fmw/iam/idmtools/bin/idmConfigTool.sh -preConfigIDStore
   ```

```
input_file=/scratch/orcl/dw_users/extend.props
Enter ID Store Bind DN password :
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_acl_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/systemid_pwdpolicy.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idstore_tuning.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schema_extn.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_pwd_
schema_add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oim_pwd_schema_
add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
add.ldif
May 25, 2011 2:37:34 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
index_add.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them. The file with the name **automation.log** is created in the directory from where you run the tool.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.4.2 Creating Users and Groups for Oracle Access Manager

If you plan to implement Oracle Access Manager in your topology, you must seed the Identity Store with users that are required by Oracle Access Manager.

To do this, perform the following tasks on IDMHOST1

1. Set the Environment Variables: MW_HOME, JAVA_HOME, IDM_HOME and ORACLE_HOME.

   Set IDM_HOME to IDM_ORACLE_HOME.

   Set ORACLE_HOME to IAM_ORACLE_HOME.

2. Create a properties file, called oam.props with the following contents:

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
```

```
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
IDSTORE_OAMSOFTWAREUSER:oamLDAP
IDSTORE_OAMADMINUSER:oamadmin
```

Where:

- `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store Directory.

- `IDSTORE_BINDDN` is an administrative user in the Identity Store Directory.

- `IDSTORE_USERSEARCHBASE` is the location in the directory where Users are Stored.

- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are Stored.

- `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

- `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity Stores are in the same directory. If not, it is set to `false`.

- `OAM11G_IDSTORE_ROLE_SECURITY_ADMIN` is the name of the group which is used to allow access to the OAM console.

- `IDSTORE_OAMADMINUSER` is the name of the user you want to create as your Oracle Access Manager Administrator.

- `IDSTORE_OAMSOFTWAREUSER` is a user that gets created in LDAP that is used when Oracle Access Manager is running to connect to the LDAP server.

3. Configure the Identity Store by using the command `idmConfigTool`, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

   Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

   IAM_ORACLE_HOME/idmtools/bin

   The syntax of the command on Linux is:

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

   The syntax on Windows is:

   ```
   idmConfigTool.bat -prepareIDStore mode=OAM input_file=configfile
   ```

   For example:

   ```
   idmConfigTool.sh -prepareIDStore mode=OAM input_file=oam.props
   ```

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

Sample command output:

```
[orcl@rws3450009 dw_users]$
/u01/app/oracle/product/fmw/iam/idmtools/bin/idmConfigTool.sh -prepareIDStore
mode=OAM input_file=/scratch/orcl/dw_users/oam.props
Enter ID Store Bind DN password :
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
schema_extn.ldif
*** Creation of Oblix Anonymous User ***
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
10g_anonymous_user_template.ldif
Enter User Password for oblixanonymous:
Confirm User Password for oblixanonymous:
*** Creation of oamadmin ***
May 25, 2011 2:45:08 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamadmin:
Confirm User Password for oamadmin:
*** Creation of oamLDAP ***
May 25, 2011 2:45:16 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamLDAP:
Confirm User Password for oamLDAP:
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/common/oam_user_group_read_
acl_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_
group_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
group_member_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
config_acl.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schemaadmin.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them. The file with the name automation.log is created in the directory from where you run the tool.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the idmConfigTool command.

11.4.3 Creating Users and Groups for Oracle Identity Manager

If you plan to implement Oracle Identity Manager in your topology, you must seed the Identity Store with the xelsysadm user and assign it to an Oracle Identity Manager

administrative group. You must also create a user outside of the standard `cn=Users` location to be able to perform reconciliation. This user is also the user that should be used as the bind DN when connecting to directories with Oracle Virtual Directory.

> **Note:** This command also creates a container in your Identity Store for reservations.

To do this, perform the following tasks on `IDMHOST1`:

1. Set the Environment Variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.

2. Create a properties file, called `oim.props`, with the following contents:

   ```
   IDSTORE_HOST : idstore.mycompany.com
   IDSTORE_PORT : 389
   IDSTORE_BINDDN : cn=orcladmin
   IDSTORE_USERNAMEATTRIBUTE: cn
   IDSTORE_LOGINATTRIBUTE: uid
   IDSTORE_USERSEARCHBASE:cn=Users,dc=mycompany,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=us,dc=oracle,dc=com
   IDSTORE_SEARCHBASE: dc=mycompany,dc=com
   POLICYSTORE_SHARES_IDSTORE: true
   IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
   IDSTORE_OIMADMINUSER: oimadmin
   IDSTORE_OIMADMINGROUP:OIMAdministrators
   ```

   Where:

   - `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory.

   - `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.

   - `IDSTORE_OIMADMINUSER` is the name of the administration user you would like to use to log in to the Oracle Identity Manager console.

   - `IDSTORE_OIMADMINGROUP` Is the name of the group you want to create to hold your Oracle Identity Manager administrative users.

   - `IDSTORE_USERSEARCHBASE` is the location in your Identity Store where users are placed.

   - `IDSTORE_GROUPSEARCHBASE` is the location in your Identity Store where groups are placed.

   - `IDSTORE_SYSTEMIDBASE` is the location in your directory where the Oracle Identity Manager reconciliation user are placed.

   - `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity stores are in the same directory. If not, it is set to `false`.

3. Configure the Identity Store by using the command `idmConfigTool`, which is located at: *IAM_ORACLE_HOME*/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command on Linux is:

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

The syntax on Windows is:

```
idmConfigTool.bat -prepareIDStore mode=OIM input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=oim.props
```

When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to the accounts:

- `IDSTORE_OIMADMINUSER`

- `xelsysadm` (It is recommended you set this to the same value as the account you create as part of the Oracle Identity Manager configuration.)

Sample command output:

```
Enter ID Store Bind DN password :
*** Creation of oimadmin ***
Apr 5, 2011 4:58:51 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oim_user_template.ldif
Enter User Password for oimadmin:
Confirm User Password for oimadmin:
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oim_group_template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oim_group_member_
template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oim_groups_acl_
template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oim_reserve_
template.ldif
*** Creation of Xel Sys Admin User ***
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oam_user_template.ldif
Enter User Password for xelsysadm:
Confirm User Password for xelsysadm:
The tool has completed its operation. Details have been logged to
/home/oracle/idmtools/oim.log
```

4. Check the log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory from where you run the tool.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.4.4 Creating Users and Groups for Oracle WebLogic Server

When you enable single sign-on for your administrative consoles, you must ensure that there is a user in your Identity Store that has the permissions to log in to your WebLogic Administration Console and Oracle Enterprise Manager Fusion Middleware Control.

To do this, perform the following tasks on `IDMHOST1`:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.

2. Create a properties file, called `wls.props` with the following contents:

   ```
   IDSTORE_HOST: idstore.mycompany.com
   IDSTORE_PORT: 389
   IDSTORE_BINDDN: cn=orcladmin
   IDSTORE_USERNAMEATTRIBUTE: cn
   IDSTORE_LOGINATTRIBUTE: uid
   IDSTORE_USERSEARCHBASE: cn=Users, dc=mycompany,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
   IDSTORE_SEARCHBASE: dc=mycompany,dc=com
   POLICYSTORE_SHARES_IDSTORE: true
   ```

   Where:

   - `IDSTORE_HOST` and IDSTORE_PORT are, respectively, the host and port of your Identity Store Directory.

   - `IDSTORE_BINDDN` Is an administrative user in the Identity Store directory.

   - `IDSTORE_USERSEARCHBASE` is the location in the directory where Users are Stored.

   - `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are Stored.

   - `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

   - `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity Stores are in the same directory. If not, it is set to `false`.

   The command creates a user called `weblogic_idm` and assigns it to a group called `IDM Administrators`.

3. Configure the Identity Store by using the command `idmConfigTool`, which is located at *IAM_ORACLE_HOME*/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command on Linux is:

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

The syntax on Windows is:

```
idmConfigTool.bat -prepareIDStore mode=WLS input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=wls.props
```

When the command runs you are prompted to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to the account `weblogic_idm`.

Sample command output:

```
Enter ID Store Bind DN password :
*** Creation of Weblogic Admin User ***
Apr 5, 2011 5:52:04 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oam_user_template.ldif
Enter User Password for weblogic_idm:
Confirm User Password for weblogic_idm:
Apr 5, 2011 5:52:12 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/weblogic_admin_
group.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.4.5 Creating Users and Groups for Fusion Applications

Oracle Fusion Applications requires several users and groups to be created in the Identity Store.

To do this perform the following tasks on `IDMHOST1`:

1. Set the Environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.

2. Create a properties file, called `fusion.props` with the following contents:

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_USERSEARCHBASE:cn=Users,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycomapny,dc=com
IDSTORE_SUPERUSER: weblogic_fa
POLICYSTORE_SHARES_IDSTORE: true
```

Where:

- `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory.

- `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.

- `IDSTORE_READONLYUSER` is the name of a user you want to create which has Read Only permissions on your Identity Store.

- `IDSTORE_READWRITEUSER` is the name of a user you want to create which has Read/Write permissions on your Identity Store.

- `IDSTORE_SUPERUSER` is the name of the administration user you want to use to log in to the WebLogic Administration Console in the Oracle Fusion Applications domain.

- `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity stores are in the same directory. If not, it is set to `false`.

In addition to creating the users, the command also creates the following groups:

- `orclFAGroupReadPrivilegeGroup`

- `orclFAGroupWritePrivilegeGroup`

- `orclFAUserReadPrivilegeGroup`

- `orclFAUserWritePrefsPrivilegeGroup`

- `orclFAUserWritePrivilegeGroup`

3. Configure the Identity Store by using the command `idmConfigTool`, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

   > **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
   >
   > *IAM_ORACLE_HOME*/idmtools/bin

   The syntax of the command on Linux is:

   `idmConfigTool.sh -prepareIDStore mode=fusion input_file=`*configfile*

   The syntax on Windows is:

   `idmConfigTool.bat -prepareIDStore mode=fusion input_file=`*configfile*

For example:

```
idmConfigTool.sh -prepareIDStore mode=fusion input_file=fusion.props
```

The command prompts you to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to the accounts:

- `IDSTORE_READONLYUSER`

- `IDSTORE_READWRITEUSER`

Sample command output:

```
Enter ID Store Bind DN password :
*** Creation of IDROUser ***
Apr 5, 2011 9:05:52 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oam_user_template.ldif
Enter User Password for IDROUser:
Confirm User Password for IDROUser:
*** Creation of IDRWUser ***
Apr 5, 2011 9:06:00 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/oid/oam_user_template.ldif
Enter User Password for IDRWUser:
Confirm User Password for IDRWUser:
Apr 5, 2011 9:06:08 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/common/oam_user_read_acl_
template.ldif
Apr 5, 2011 9:06:08 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/IAM/idmtools/templates/common/oam_user_read_write_
acl_template.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them.

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.4.6 Creating Access Control Lists in Non-Oracle Internet Directory Directories

In the preceding sections, you seeded the Identity Store with users and artifacts for the Oracle components. If your Identity Store is hosted in a non-Oracle Internet Directory directory, such as Microsoft Active Directory, you must set up the access control information (ACIs) to provide appropriate privileges to the entities you created. This section lists the artifacts on which the ACIs need to be set.

- Users and groups. ACIs to the users and groups container are provided in Oracle Internet Directory. Set them manually for other directories. The Oracle Identity Manager/Oracle Access Manager integration and Fusion Applications require the following artifacts to be created in the Identity store.

  – Group with read privileges to the users container (`orclFAUserReadPrivilegeGroup`)

- – Group with read/write privileges to the users container
  (`orclFAUserWritePrivilegeGroup`)

- – Group with read privileges to the groups container
  (`orclFAGroupReadPrivilegeGroup`)

- – Group with read privileges to the groups container
  (`orclFAGroupWritePrivilegeGroup`)

- – Group with write privileges to a partial set of attributes
  (`orclFAUserWritePrefsPrivilegeGroup`)

- The user specified by the `IDSTORE_READONLYUSER` parameter. It is assigned to the groups `orclFAUserReadPrivilegeGroup` and `orclFAGroupReadPrivilegeGroup`.

- The user specified by the `IDSTORE_READWRITEUSER` parameter. It is assigned to the groups `orclFAUserWritePrivilegeGroup` and `orclFAGroupWritePrivilegeGroup`.

- The user specified by `IDSTORE_READONLYUSER`. It is assigned to `OrclFAUserWritePrefPrivilegeGroup`.

- Systemids. The System ID container is created for storing all the system identifiers. If there is another container in which the users are to be created, that is specified as part of the admin.

- Oracle Access Manager Admin User

- Oracle Access Manager Software User. This is added to the groups where the user gets read privileges to the container. This is also provided with schema admin privileges.

- Oracle Identity Manager user under System ID container. Password policies are set accordingly in the container.

- Oracle Identity Manager administration group. The Oracle Identity Manager user is added as its member. The Oracle Identity Manager admin group is given complete read/write privileges to all the user and group entities in the directory.

- Reserve container. Permissions are provided to the Oracle Identity Manager admin group to perform read/write operations.

11.4.7 Updating Oracle Virtual Directory Adapters

Oracle recommends that, after creating the artifacts in the Identity Store, you update the Oracle Virtual Directory adapters you set up in Section 9.8, "Creating Adapters in Oracle Virtual Directory" so that they have a less privileged user. The following procedure is recommended, but not mandatory.

Change the value of Server Proxy Bind DN to
`cn=oimAdmin,cn=systemids,dc=mycompany,dc=com`.

To do this, perform the following steps:

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:
   `http://admin.mycompany.com/odsm`.

2. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.

3. On the Home page, click the **Adapter** tab.

4. Click **User Adapter**.

5. On the General tab in the **Credential Processing** section, make the following changes:

    ▪   **Proxy DN**: `cn=oimAdmin,cn=systemids,dc=mycompany,dc=com`

    ▪   **Proxy Password**: The password of the **Proxy DN** account.

6. Click **Apply**.

7. Click **Change Log Adapter**.

8. On the General tab in the **Credential Processing** section, make the following changes:

    ▪   **Proxy DN**: `cn=oimAdmin,cn=systemids,dc=mycompany,dc=com`

    ▪   **Proxy Password**: The password of the **Proxy DN** account.

9. Click **Apply**.

10. Click the **Plug-Ins** tab.

11. Click **Changelog Plug-in**.

12. Click **Edit**.

13. Change **ModifierDNFilter** to:

    `!(modifiersname=cn=oimAdmin,cn=systemids,dc=mycompany,dc=com)`

14. Click **OK**.

15. Click **Apply**.

16. Repeat for each Oracle Virtual Directory connection.

12

Extending the Domain with Oracle Access Manager 11g

This chapter describes how to install and configure Oracle Access Manager 11.1.1 for use in the Oracle Identity Management enterprise deployment.

This chapter includes the following topics:

12.1 Introduction to Installing Oracle Access Manager

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

Oracle Access Manager consists of various components, including Access Server, Access Manager Console, and WebGates. The Access Server, which includes both the Access Server and Identity Server, are the server components necessary to serve user requests for access to enterprise resources. The Access Manager console is the administrative console to the Access Server. WebGates are web server agents that act as the actual enforcement points for Oracle Access Manager. Follow the instructions in this chapter and Chapter 18, "Configuring Single Sign-on for Administration Consoles"

to install and configure the Oracle Access Manager components necessary for your enterprise deployment.

This section contains the following topics:

- Section 12.1.1, "Using Different LDAP Directory Stores"
- Section 12.1.2, "Using Oracle Virtual Directory as the Identity Store"

12.1.1 Using Different LDAP Directory Stores

The enterprise deployment described in this guide shows Oracle Access Manager using Oracle Internet Directory as the only LDAP repository. Oracle Access Manager uses a single LDAP for policy and configuration data. It is possible to configure another LDAP as the Identity Store where users, organizations and groups reside. For example, an Oracle Access Manager instance may use Oracle Internet Directory as its policy and configuration store and point to an instance of Microsoft Active Directory for users and groups.

12.1.2 Using Oracle Virtual Directory as the Identity Store

In addition, the Identity Stores can potentially be front-ended by Oracle Virtual Directory to virtualize the data sources.

To learn more about the different types of directory configuration for Oracle Access Manager, consult the 11*g* Oracle Access Manager documentation at Oracle Technology Network. Customers considering these variations should adjust their directory tier and Oracle Access Manager deployment accordingly.

12.2 Prerequisites

Before you configure Oracle Access Manager, ensure that the following tasks have been performed on IDMHOST1 and IDMHOST2:

1. Install Oracle WebLogic Server as described in Section 4.5.3.
2. Install Identity Management as described in Section 4.5.4.
3. Install Oracle Identity and Access Management as described in Section 4.5.7.
4. Install the Identity Store, as described in Chapter 7, "Extending the Domain with Oracle Internet Directory" or Chapter 10, "Preparing Directories Other than Oracle Internet Directory."
5. Install Oracle Virtual Directory, if required, as described in Chapter 9, "Extending the Domain with Oracle Virtual Directory."

12.3 Configuring Oracle Access Manager on IDMHOST1

This section contains the following topics:

- Section 12.3.1, "Extending Domain with Oracle Access Manager"
- Section 12.3.2, "Removing IDM Domain Agent"
- Section 12.3.3, "Propagating the Domain Changes to the Managed Server Domain Directory"

12.3.1 Extending Domain with Oracle Access Manager

Start the configuration wizard by executing the command:

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 WebLogic Administration Server, for example: *ORACLE_ BASE*/admin/*IDMDomain*/aserver/*IDMDomain*.

   Click **Next**

3. On the Select Extension Source screen, select **Oracle Access Manager with Database Policy Store**.

   Click **Next**

4. The schedulerDS Multi Data Source is shown the Configure RAC Multi Data Sources screen, if you have Oracle Directory Integration Platform configured in your domain. Do not make any changes to this data source.

   Click **Next**.

5. On the Configure JDBC Component Schema screen select the datasource **OAM Infrastructure**.

   Select **Configure selected data sources as RAC multi data sources** in the next panel.

   Click **Next**.

6. On the Configure RAC Multi Data Sources Screen:

   - **Service Name**: Service name of the database that contains the Oracle Access Manager repository (oamedg.mycompany.com)

   - **User Name**: EDG_OAM

   - **Password**: Password for user EDG_OAM

   In the top right box, click **Add** to add the second Oracle RAC node.

   - **Host Name**: OIDDBHOST1-VIP

   - **Instance Name**: idmdb1

   - **Port**: 1521

   Click **Add** again to add the second database host:

   - **Host Name**: OIDDBHOST2-VIP

   - **Instance Name**: idmdb2

   - **Port**: 1521

   If you are using Oracle Database 11.2, replace the vip addresses with the 11.2 SCAN address.

   Click **Next**.

7. On the Test Component Schema screen, the Wizard attempts to validate the data sources. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the problem, and try again.

8. On the Select Optional Configuration screen, select **Managed Servers, Clusters and Machines**.

   Click **Next**

9. When you first enter the Configure Managed Servers screen, the configuration wizard creates a default Managed Server for you. AT this point, you must do two things:

   a. Change the values of the default Managed Server.

   b. Add a second Managed Server and supply values for it.

   That is, you must *change the existing 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.

   For the default Oracle Access Manager server (oam_server) entry, *change* the following values:

   - **Name**: WLS_OAM1

   - **Listen Address**: IDMHOST1

   To add the second Oracle Access Manager Server, click **Add** and supply the following values:

   - **Name**: WLS_OAM2

   - **Listen Address**: IDMHOST2

   - **Listen Port**: 14100

   Leave all the other fields at the default settings.

   Click **Next**.

10. On the Configure Clusters screen, create a cluster by clicking **Add**. Supply the following information:

    - **Name**: cluster_oam

    - **Cluster Messaging Mode**: unicast

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

11. 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.

    The cluster_oam has the Managed Servers WLS_OAM1 and WLS_OAM2.

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

    Click **Next**.

12. On the Configure Machines screen, create a machine for each host in the topology. Click the tab **UNIX** if your hosts use Linux or a UNIX-based operating system. Otherwise, click **machines**. Supply:

    - **Name**: The name of the host. Best practice is to use the DNS name. For example: idmhost1.mycompany.com and idmhost2.mycompany.com for the first and second nodes respectively.

    - **Node Manager Listen Address**: The DNS name of the machine. For example: idmhost1.mycompany.com and idmhost2.mycompany.com for the first and second nodes respectively.

- **Node Manager Port**: A port for Node Manager to use.

  If you have already configured Oracle Directory Integration Platform or ODSM, machines already exist for those hosts.

  Click **Next**.

13. On the Assign Servers to Machines screen, indicate which Managed Servers to run on each of the machines you created.

    Click a machine in the right pane.

    Click the Managed Servers you want to run on that machine in the left pane.

    Click the arrow to assign the Managed Servers to the machines. Repeat until all Managed Servers are assigned to machines. For example:

    IDMHOST1: **WLS_OAM1**

    IDMHOST2: **WLS_OAM2**

    Click **Next** to continue.

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

    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.

    ---

15. On the Installation Complete screen, click **Done**.

16. Restart WebLogic Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

12.3.2 Removing IDM Domain Agent

By default, the IDMDomain Agent provides single sign-on capability for administration consoles. In enterprise deployments, WebGate handles single sign-on, so you must remove the IDMDomain agent. Remove the IDMDomain Agent as follows:

Log in to the WebLogic console using the URL:
`http://admin.mycompany.com/console`

 Then:

1. Select **Security Realms** from the **Domain Structure** Menu

2. Click **myrealm**.

3. Click the **Providers** tab.

4. Click **Lock and Edit** from the **Change Center**.

5. In the list of authentication providers, select **IAMSuiteAgent**.

6. Click **Delete**.

7. Click **Yes** to confirm the deletion.

8. Click **Activate Changes** from the **Change Center**.

9. Restart WebLogic Adminisration Server and ALL running Managed Servers, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

10. Start the WebLogic Managed Server `WLS_OAM1` as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

12.3.3 Propagating the Domain Changes to the Managed Server Domain Directory

To propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory, proceed as follows:

1. Run the pack command on `IDMHOST` to create a template pack. Type the following commands:

```
IDMHOST1> cd MW_HOME/oracle_common/common/bin
IDMHOST1> ./pack.sh -managed=true -domain=ORACLE_
BASE/admin/IDMDomain/aserver/IDMDomain -template=MW_
HOME/templates/IDMDomain.jar -template_name=IDMDomain_Template
```

2. Run the unpack command on `IDMHOST1` to unpack the propagated template to the domain directory of the Managed Server. Type the following command:

```
IDMHOST1> ./unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain/
-template=MW_HOME/templates/IDMDomain.jar -overwrite_domain=true -app_
dir=ORACLE_BASE/admin/IDMDomain/mserver/applications
```

3. Restart Managed Server `WLS_OAM1`.

12.4 Configuring Oracle Access Manager on IDMHOST2

This section contains the following topics:

- Section 12.4.1, "Deploying Oracle Access Manager on IDMHOST2"

- Section 12.4.2, "Updating Node Manager Properties File on IDMHOST2"

- Section 12.4.3, "Starting Oracle Access Manager Server on IDMHOST2"

12.4.1 Deploying Oracle Access Manager on IDMHOST2

Once the configuration has succeeded on `IDMHOST1`, you can propagate the configuration to `IDMHOST2`. You do this by packing the domain on `IDMHOST1`, using the pack script, and unpacking it on `IDMHOST2` using the unpack script. Both scripts reside in `MW_HOME/oracle_common/common/bin`.

In Step 1 of Section 12.3.3, "Propagating the Domain Changes to the Managed Server Domain Directory," you created a file called `IDMDomain.jar` in the `MW_HOME/templates` directory. Copy this file to `IDMHOST2`.

Unpack the file on `IDMHOST2` by using the `unpack` utility:

```
./unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain -template=MW_
HOME/templates/IDMDomain.jar -overwrite_domain=true -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

12.4.2 Updating Node Manager Properties File on IDMHOST2

If the Node Manager is not already started on `IDMHOST2`, perform the following steps to start it:

1. Start the Node Manager on `IDMHOST2` to create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the *MW_HOME*/`wlserver_10.3/server/bin` directory.

2. Before you can start the Managed Servers by using the console, node manager requires that the property `StartScriptEnabled` is set to `true`. You set it by running the `setNMProps.sh` script located under the *MW_HOME*/`oracle_common/common/bin` directory.

   ```
   prompt>  MW_HOME/oracle_common/common/bin
   prompt> ./setNMProps.sh
   ```

3. Stop and Start the Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components"so that the properties take effect.

12.4.3 Starting Oracle Access Manager Server on IDMHOST2

Start Oracle Access Manager on `IDMHOST2` by following the start procedures in Section 19.1, "Starting and Stopping Oracle Identity Management Components" for:

- Node Manager (if it is not already started)
- WebLogic Managed Server `WLS_OAM2`

12.5 Configuring Oracle Access Manager to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier.

This section contains the following topics:

- Section 12.5.1, "Prerequisites"
- Section 12.5.2, "Configuring Oracle HTTP Servers to Display Login Page"
- Section 12.5.3, "Configuring Oracle HTTP Servers to Access Oracle Access Manager Console"
- Section 12.5.4, "Validating Accessibility"

12.5.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Configure Oracle Web Tier on `WEBHOST1` and `WEBHOST2` as described in Section 5.1, "Configuring the Oracle Web Tier."

2. Configure Oracle Access Manager on `IDMHOST1` and `IDMHOST2` as described in Section 12.3, "Configuring Oracle Access Manager on IDMHOST1" and Section 12.4, "Configuring Oracle Access Manager on IDMHOST2."

3. Configure the load balancer with a virtual host name (`sso.mycompany.com`) routing traffic to the webservers on `WEBHOST1` and `WEBHOST2` as described in Section 2.2.2, "Configuring Virtual Server Names and Ports on the Load Balancer."

4. Configure the load balancer with a virtual host name (admin.mycompany.com) routing traffic to webservers WEBHOST1 and WEBHOST2 Section 2.2.2, "Configuring Virtual Server Names and Ports on the Load Balancer."

12.5.2 Configuring Oracle HTTP Servers to Display Login Page

On each of the web servers on WEBHOST1 and WEBHOST2 create a file called oam.conf in the directory *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf.

This file must contain the following information:

```
<Location /oam>
    SetHandler weblogic-handler
    WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>
```

It must also contain:

```
<Location /fusion_apps>
    SetHandler weblogic-handler
    WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>
```

if the END user uses the FAAuthScheme to protect its Application Domain, that is, the FusionApplication.

12.5.3 Configuring Oracle HTTP Servers to Access Oracle Access Manager Console

On each of the web servers on WEBHOST1 and WEBHOST2, a file called admin.conf was created in the directory *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf. (See Section 6.9, "Configuring Oracle HTTP Server for the WebLogic Administration Server".) Edit this file and add the following lines within the virtual host definition:

```
<Location /oamconsole>
   SetHandler weblogic-handler
   WebLogicHost ADMINVHN
   WebLogicPort 7001
</Location>
```

After editing the file should look like:

```
NameVirtualHost *:80

<VirtualHost *:80>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
    RewriteRule ^/console/jsp/common/logout.jsp /oamsso/logout.html [PT]
    RewriteRule ^/em/targetauth/emaslogout.jsp /oamsso/logout.html [PT]

    # Admin Server and EM
    <Location /console>
       SetHandler weblogic-handler
       WebLogicHost ADMINVHN
       WeblogicPort 7001
    </Location>

    <Location /consolehelp>
       SetHandler weblogic-handler
```

```
      WebLogicHost ADMINVHN
      WeblogicPort 7001
   </Location>

   <Location /em>
      SetHandler weblogic-handler
      WebLogicHost ADMINVHN
      WeblogicPort 7001
   </Location>

   <Location /oamconsole>
      SetHandler weblogic-handler
      WebLogicHost ADMINVHN
      WebLogicPort 7001
   </Location>

</VirtualHost>
```

Restart the Oracle HTTP Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

12.5.4 Validating Accessibility

Attempt to access the Oracle Access Manager application using the URL:
`https://sso.mycompany.com/oam`

The Oracle Access Manager screen is displayed. A message saying `Action Failed` appears on the screen. You can ignore the message because all you are testing is that the Oracle Access Manager server can be accessed through the Load Balancer.

Attempt to Access the OAM console at:
`http://admin.mycompany.com/oamconsole`

12.6 Configuring Oracle Access Manager

This section contains the following topics:

- Section 12.6.1, "Changing Oracle Access Manager Security Model"
- Section 12.6.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool"
- Section 12.6.3, "Validating the Configuration"

12.6.1 Changing Oracle Access Manager Security Model

By default, Oracle Access Manager is configured to use the Open security model. Many applications require a different security model with a higher level of security.

If you want to change the security model, proceed as follows:

Log in to the OAM console at:

`http://admin.mycompany.com/oamconsole`

as the WebLogic administration user. Then perform the following steps:

1. Click the **System Configuration** tab.

2. Expand **Server Instances** under the Common Configuration section.

3. Click an Oracle Access Manager server, for example, **WLS_OAM1**, then select **Open** from the **Actions** menu.

4. Change the mode to the required security model, for example, **Simple**.

5. Click **Apply**.

6. The Confirm Edit dialog appears:

    ```
    OAM Server instance wls_oam1 might be in use, are you sure you want to edit it?
    ```

    Select **Yes**.

7. Repeat for each Oracle Access Manager server.

8. Click **Access Manager Settings** located in the Access Manager Settings section.

9. Select **Open** from the **Actions** menu. The access manager settings are displayed.

10. If you have changed the security mode to Simple, supply a global passphrase.

    If you have changed the security mode to Cert Mode Configuration, provide the keystore details.

11. Click **Apply**.

12. Click the **System Configuration** tab.

13. Expand **Access Manager Settings - SSO Agents**.

14. Click **OAM Agents** and select **Open** from the **Actions** menu.

15. In the Search window, click **Search**.

16. Click **IAMSuiteAgent** in the search results. The Agent Properties are displayed.

17. Set the Security value to the new security model.

    Click **Apply**.

18. Restart the managed servers WLS_OAM1 and WLS_OAM2 as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

> **Note:** The Simple Security model is recommended if you plan to run Oracle Fusion Applications

---

12.6.2 Configuring Oracle Access Manager by Using the IDM Automation Tool

Now that the initial installation is done and the security model set, the following tasks must be performed:

- Oracle Access Manager must be configured to use an external LDAP Directory (idstore.mycompany.com).

- Oracle Access Manager WebGate Agent must be created.

- You perform these tasks by using idmConfigTool.

Perform the following tasks on IDMHOST1:

1. Set the environment variables MW_HOME, JAVA_HOME, IDM_HOME and ORACLE_HOME.

    Set IDM_HOME to IDM_ORACLE_HOME.

    Set ORACLE_HOME to IAM_ORACLE_HOME.

2. Create a properties file called config_oam1.props with the following contents:

```
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: oamhost1.mycompany.com:5575,oamhost2.mycompany.com:5575
WEBGATE_TYPE: ohsWebgate10g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.mycompany.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
OAM_TRANSFER_MODE: simple
COOKIE_DOMAIN: .mycompany.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: false
OAM11G_IMPERSONATION_FLAG:true
OAM11G_SERVER_LBR_HOST:sso.mycompany.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
OAM11G_OIM_WEBGATE_PASSWD: password to be assigned to WebGate
COOKIE_EXPIRY_INTERVAL: 120
```

Where:

- ■ `WLSHOST` and `WLSPORT` are, respectively, the host and port of your administration server. This is the virtual name.

- ■ `WLSADMIN` is the WebLogic administrative user you use to log in to the WebLogic console.

- ■ `IDSTORE_HOST` and `IDSTORE _PORT` are, respectively, the host and port of your Identity Store directory.

- ■ `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.

- ■ `IDSTORE_USERSEARCHBASE` is the location in the directory where Users are stored.

- ■ `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are stored.

- ■ `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

- ■ `IDSTORE_OAMSOFTWAREUSER` is the name of the user you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager" to be used to interact with LDAP.

- `IDSTORE_OAMADMINUSER` is the name of the user you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager" to access your OAM Console.

- `PRIMARY_OAM_SERVERS` is a comma separated list of your Oracle Access Manager Servers and the proxy ports they use.

> **Note:** To determine the proxy ports your OAM Servers use:
>
> 1. Log in to the OAM console at
>   `http://admin.mycompany.com/oamconsole`
> 2. Click the **System Configuration** tab.
> 3. Expand **Server Instances** under the Common Configuration section
> 4. Click an Oracle Access Manager server, such as **WLS_OAM1**, and select **Open** from the **Actions** menu.
> 5. Proxy port is the one shown as **Port**.

- `ACCESS_GATE_ID` is the name you want to assign to the WebGate.

- `OAM11G_OIM_WEBGATE_PASSWD` is the password to be assign to the WebGate.

- `OAM11G_IDM_DOMAIN_OHS_HOST` is the name of the load balancer which is in front of the OHS's.

- `OAM11G_IDM_DOMAIN_OHS_PORT` is the port that the load balancer listens on.

- `OAM11G_IDM_DOMAIN_OHS_PROTOCOL` is the protocol to use when directing requests at the load balancer.

- `OAM11G_WG_DENY_ON_NOT_PROTECTED`, when set to `false`, allows login pages to be displayed.

- `OAM_TRANSFER_MODE` is the security model that the Access Servers function in, as defined in Section 12.6.1, "Changing Oracle Access Manager Security Model."

- `OAM11G_OAM_SERVER_TRANSFER_MODE` is the security model that the Access Servers function in, as defined in Section 12.6.1, "Changing Oracle Access Manager Security Model."

- `OAM11G_IMPERSONATION_FLAG` is set to `True` if you are using Oracle Fusion Applications.

- `OAM11G_IDM_DOMAIN_LOGOUT_URLS` is set to the various logout URLs.

- `OAM11G_SSO_ONLY_FLAG` confgures Oracle Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization.

  If `OAM11G_SSO_ONLY_FLAG` is `true`, the Oracle Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Oracle Access Manager server.

  If the value is `false`, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Oracle

Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Oracle Access Manager server.

- `OAM11G_SERVER_LBR_HOST` is the name of the load balancer fronting your site. This and the following two parameters are used to construct your login URL.

- `OAM11G_SERVER_LBR_PORT` is the port that the load balancer is listening on.

- `OAM11G_SERVER_LBR_PROTOCOL` is the URL prefix to use.

- `COOKIE_DOMAIN` is the domain in which the WebGate functions.

- `WEBGATE_TYPE` is the type of WebGate agent you want to create.

- `OAM11G_IDSTORE_NAME` is the Identity Store name. If you already have an Identity Store in place which you wish to reuse (rather than allowing the tool to create a new one for you), then set the value of this parameter to the name of the Identity Store you wish to reuse.

3. Configure Oracle Access Manager using the command `idmConfigTool` which is located at:

IAM_ORACLE_HOME/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOAM input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -configOAM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOAM input_file=config_oam1.props
```

When the command runs you are prompted to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to these accounts:

- IDSTORE_PWD_OAMSOFTWAREUSER

- IDSTORE_PWD_OAMADMINUSER

Sample command output:

```
Enter ID Store Bind DN password :
Enter User Password for WLSPASSWD:
Confirm User Password for WLSPASSWD:
Enter User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Confirm User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Enter User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Confirm User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Enter User Password for IDSTORE_PWD_OAMADMINUSER:
```

```
Confirm User Password for IDSTORE_PWD_OAMADMINUSER:
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them. A file named `automation.log` is created in the directory where you run the tool.

5. Restart WebLogic Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

> **Note:** After you run `idmConfigTool`, several files are created that you need for subsequent tasks. Keep these in a safe location.
>
> The following files exist in the directory *DOMAIN_HOME*`/output/Webgate_IDM`. You need these when you install the WebGate software.
>
> - `ObAccessClient.xml`
> - `logout.html`

12.6.3 Validating the Configuration

To Validate that this has completed correctly.

1. Access the OAM console at:

   `http://admin.mycompany.com/oamconsole`

2. Log in as the Oracle Access Manager Admin User you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager."

3. Click the **System Configuration** tab

4. Expand **Access Manager Settings - SSO Agents - OAM Agents**.

5. Click the open folder icon, then click **Search**.

6. You should see the webgate agent `Webgate_IDM`, which you created in Section 12.6.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool."

12.7 Updating Newly-Created Agent

After generating the initial configuration, you must edit the configuration and add advanced configuration entries.

1. Select **System Configuration** Tab

2. Select **Access Manager Settings - SSO Agents - OAM Agent** from the directory tree. Double-click or select the open folder icon.

3. On the displayed search page click **Search** to perform an empty search.

4. Click the Agent `Webgate_IDM`.

5. Select **Open** from the Actions menu.

6. Update the following information:

   - **Deny if not Protected**: Deselect.

   - Set **Max Connections** to 4 for all of the Oracle Access Manager servers listed in the primary servers list.

7. Click **Apply**.

8. Click **Policy Configuration** tab.

9. Double Click **IAMSuiteAgent** under **Host Identifiers**.

10. Click **+** in the **operations** box.

11. Enter the following information:

- **Host Name**: `admin.mycompany.com`

- **Port**: `80`

12. Click **Apply**.

12.8 Validating Oracle Access Manager

You can validate Oracle Access Manager by using the `oamtest` tool. To do this, perform the following steps:

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:

`IAM_HOME`/`oam/server/tester`

4. Start the test tool in a terminal window using the command:

```
java -jar oamtest.jar
```

5. When the OAM test tool starts, enter the following information in the **Server Connection** section of the page:

- **Primary IP Address**: `idmhost1.mycompany.com`

- **Port**: `5575`

- **Agent ID**: `Webgate_IDM`

- **Agent Password**: `webgate password`

Note: if you configured simple mode, you must select **Simple** and provide the global passphrase.

Click **Connect**.

In the status window you see:

```
[reponse] Connected to primary access server
```

6. In the **Protected Resource URI** section enter:

- **Scheme**: `http`

- **Host**: `admin.mycompany.com`

- **Port**: `80`

- **Resource**: `/oamconsole`

Click **Validate**.

In the status widow you see:

```
[request][validate] yes
```

7. In the **User Identity** window, enter:

   - **Username** : `oamadmin`

   - **Password**: *oamadmin password*

   Click **Authenticate**.

   In the status window, you see:

   ```
   [response][authenticate] yes
   ```

   Click **Authorize**.

   In the status window you see.

   ```
   [response][authenticate] yes
   ```

The following is an example of a test:
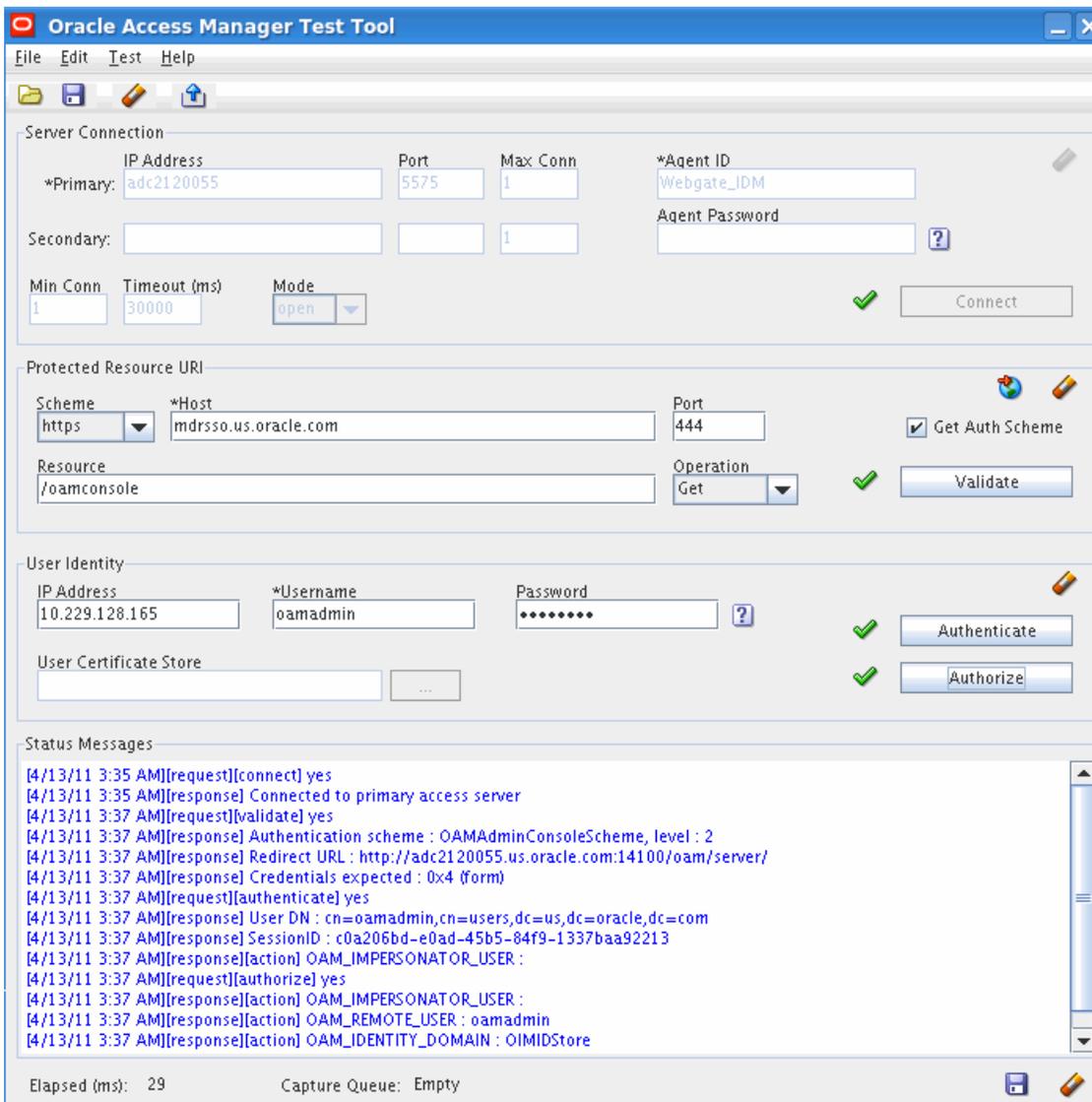
Repeat this test for each access server in the topology, remembering to change the connection details for each server.

12.9 Creating Oracle Access Manager Key Store

If you are integrating other components, such as Oracle Identity Manager and Oracle Adaptive Access Manager, with Oracle Access Manager and Oracle Access Manager is using the simple security transport model, you must generate a keystore that can be used with those components. The procedure to do this is outlined in this section. Run it on `IDMHOST1`.

This section contains the following topics:

- Section 12.9.1, "Creating an Empty Trust Store File Named oamclient-truststore.jks"
- Section 12.9.2, "Importing the CA Certificate into the Trust Store"
- Section 12.9.3, "Setting up Keystore with the SSL Certificate and Private Key file of the Access Client"

12.9.1 Creating an Empty Trust Store File Named oamclient-truststore.jks

To create this file, you use a tool called `keytool` that comes with the JDK (Java Development Kit).

Before running any of the following commands, ensure that the JDK is in your path. For example

```
export JAVA_HOME=MW_HOME/jrockit_160_24_D1.1.2-4
export PATH=$JAVA_HOME/bin:$PATH
```

1. First, execute the command:

```
keytool -genkey -alias alias_name -keystore PathName_to_Keystore -storetype JKS
```

The command prompts you for a keystore password. This password MUST be same as the global pass phrase used in the Oracle Access Manager server. The command also prompts for information about the user and organization. Enter relevant information.

Example:

```
keytool -genkey -alias oam -keystore oamclient-truststore.jks -storetype JKS
```

Sample output:

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: John Doe
What is the name of your organizational unit?
[Unknown]: MAA
What is the name of your organization?
[Unknown]: Oracle
What is the name of your City or Locality?
[Unknown]: Redwood Shores
What is the name of your State or Province?
[Unknown]: CA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=John Doe, OU=MAA, O=Oracle, L=Redwood Shores, ST=CA, C=US correct?
```

```
[no]: yes

Enter key password for <oam>
(RETURN if same as keystore password):
Re-enter new password:
```

2. Then execute the command:

```
keytool -delete -alias alias_name -keystore oamclient-truststore.jks -storetype
JKS
```

For example:

```
keytool -delete -alias oam -keystore oamclient-truststore.jks -storetype JKS
```

The command prompts for the keystore password you entered previously.

12.9.2 Importing the CA Certificate into the Trust Store

Oracle Access Manager 11g comes with a self-signed Certificate Authority that is used in Simple mode to issue certificates for the Access Client. This certificate must be added to the keystore you just created.

The certificate resides in the file cacert.der, which is located in the directory *IAM_ORACLE_HOME*/oam/server/config. Execute the following command to import a PEM/DER format CA certificate into the trust store. On Linux and UNIX-based systems, type:

```
keytool -importcert -file IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore PathName_to_keystore -storetype JKS
```

On Windows, type:

```
keytool -import -file IAM_ORACLE_HOME\oam\server\config\cacert.der -trustcacerts
-keystore PathName_to_keystore -storetype JKS
```

Enter keystore password when prompted.

Example:

```
keytool -importcert -file /IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore oamclient-truststore.jks -storetype JKS
```

Sample output:

```
Enter keystore password:
Owner: CN=NetPoint Simple Security CA - Not for General Use, OU=NetPoint,
O="Oblix, Inc.", L=Cupertino, ST=California, C=US
Issuer: CN=NetPoint Simple Security CA - Not for General Use, OU=NetPoint,
O="Oblix, Inc.", L=Cupertino, ST=California, C=US
Serial number: 0
Valid from: Wed Apr 01 05:57:22 PDT 2009 until: Thu Mar 28 05:57:22 PDT 2024
Certificate fingerprints:
MD5:  05:F4:8C:84:85:37:DB:E3:66:87:EF:39:E0:E6:B2:3F
SHA1: 97:B0:F8:19:7D:0E:22:6B:40:2A:73:73:1B:27:B2:7B:8D:64:82:21
Signature algorithm name: MD5withRSA
Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

12.9.3 Setting up Keystore with the SSL Certificate and Private Key file of the Access Client

An SSL certificate and private key were generated when you ran the `idmConfigTool` command in Section 12.6.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool." The SSL certificate and key are required for clients to communicate with Oracle Access Manager in Simple mode. The names of these files are, respectively, `aaa_cert.pem` and `aaa_key.pem`. They are located in the directory *DOMAIN_HOME*`/output/Webgate_IDM` on `IDMHOST1`, where *DOMAIN_HOME* is the Administration Server Domain home.

Execute the following commands to import the certificate and key file into the keystore `oamclient-keystore.jsk`.

1. Unzip the file `importcert.zip`, which is located in the directory:

   IAM_ORACLE_HOME`/oam/server/tools/importcert`

   For example:

   ```
   cd IAM_ORACLE_HOME/oam/server/tools/importcert
   unzip importcert.zip
   ```

2. Execute the command:

   ```
   openssl pkcs8 -topk8 -nocrypt -in DOMAIN_HOME/output/Webgate_IDM/aaa_key.pem
   -inform PEM -out aaa_key.der -outform DER
   ```

   The command prompts for a passphrase. Enter the password, which must be the global passphrase. This command creates the `aaa_key.der` file in the directory where the command is run

   Example:

   ```
   openssl pkcs8 -topk8 -nocrypt -in
   /u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/output/Webgate_IDM/aaa_
   key.pem -inform PEM -out aaa_key.der -outform DER
   Enter pass phrase for oamclient-truststore.jks:
   ```

3. Then execute:

   ```
   openssl x509 -in
   /u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/output/Webgate_IDM/aaa_
   cert.pem -inform PEM -out aaa_cert.der -outform DER
   ```

   This command creates the `aaa_cert.der` file in the directory where the command is run. This command does not generate any output.

4. Execute the command:

   ```
   java -cp IAM_ORACLE_HOME/oam/server/tools/importcert/importcert.jar
   oracle.security.am.common.tools.importcerts.CertificateImport -keystore
   ssoKeystore.jks -privatekeyfile aaa_key.der -signedcertfile aaa_cert.der
   -storetype jks -genkeystore yes
   ```

   This command creates the `ssoKeystore.jks` file in the directory where the command is run.

   In this command, `aaa_key.der` and `aaa_cert.der` are, respectively, the private key and certificate pair in DER format.

   Sample output:

   ```
   Enter keystore password as prompted. This MUST be same as global pass phrase.
   ```

```
The files ssoKeystore.jks  and oamclient-truststore.jks can now be used to
allow clients to connect to OAM.
```

> **Note:** The files `ssoKeystore.jks` and `oamclient-truststore.jks` are required when you integrate Oracle Access Manager running in Simple mode with Oracle Identity Management or Oracle Access Manager. When you integrate these components, you are asked to copy these files to the *DOMAIN_HOME*/`config/fmwconfig` directory. If you subsequently extend the domain on machines where these files have been placed using `pack/unpack`, you must recopy `ssoKeystore.jks` and `oamclient-truststore.jks` after unpacking.

12.10 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 5.5, "Backing up the Web Tier Configuration."

2. Back up the Oracle Access Manager 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 6.15, "Backing Up the WebLogic Domain."

4. Back up the Oracle Internet Directory as described in Section 7.7, "Backing up the Oracle Internet Directory Configuration."

5. Back up the Oracle Virtual Directory as described in Section 9.10, "Backing Up the Oracle Virtual Directory Configuration."

For information about backing up the application tier configuration, see Section 19.4, "Performing Backups and Recoveries."

13

Extending the Domain with Oracle Identity Manager

This chapter describes how to install and configure Oracle Identity Manager 11.1.1 for use in the Oracle Identity Management Enterprise Deployment Topology.

This chapter contains the following topics:

- Section 13.1, "Prerequisites"
- Section 13.2, "Enabling Virtual IP Addresses on OIMHOST1 and OIMHOST2"
- Section 13.3, "Extending the Domain to Configure Oracle Identity Manager and Oracle SOA Suite on IDMHOST1"
- Section 13.4, "Configuring Oracle Identity Manager on IDMHOST1"
- Section 13.5, "Propagating the Oracle Identity Manager and SOA Managed Servers to Oracle Identity Manager Servers"
- Section 13.6, "Post-Installation Steps on OIMHOST1"
- Section 13.7, "Post-Installation Steps on OIMHOST2"
- Section 13.8, "Modifying the Oracle Identity Manager Default System Properties for UserName Generation"
- Section 13.9, "Configuring Oracle Identity Manager to Reconcile from ID Store"
- Section 13.10, "Configuring Oracle Identity Manager to Work with the Oracle Web Tier"
- Section 13.11, "Configuring a Default Persistence Store for Transaction Recovery"
- Section 13.12, "Configuring an IT Resource Instance for Email"
- Section 13.13, "Enabling OIM to Connect to SOA Using the Administrative Users Provisioned in LDAP"
- Section 13.14, "Tuning Oracle Platform Security"
- Section 13.15, "Backing Up the Application Tier Configuration"

Oracle Identity Manager is a user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories. It also improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a standalone product or as part of Oracle Identity Management.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password

management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility through adapters.

Oracle Identity Manager provides the following key functionalities:

- User Administration
- Workflow and Policy
- Password Management
- Audit and Compliance Management
- Integration Solutions
- User Provisioning
- Organization and Role Management

For details about Oracle Identity Manager, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

13.1 Prerequisites

Before extending the domain with Oracle Identity Manager, ensure that the following tasks have been performed:

1. Ensure that the virtual IP addresses for the Oracle Identity Manager and SOA managed servers have been provisioned. See Section 2.2.3, "Virtual IP Addresses" for details

2. Install and upgrade the following software on `IDMHOST1`, `IDMHOST2`, `OIMHOST1` and `OIMHOST2`:

   - WebLogic Server: See Section 4.5.3.
   - Oracle Identity Management: See Section 4.5.4 and Section 4.5.5.
   - Oracle SOA Suite: See Section 4.5.6.
   - Oracle Identity and Access Management: See Section 4.5.7.

3. Ensure that you have created the wlfullclient.jar file, as described in Section 4.6.2, "Creating the wlfullclient.jar File."

4. Install and configure the Oracle Internet Directory instances, as described in Chapter 7.

5. If you are using Oracle Virtual Directory, ensure you have extended the domain with Oracle Virtual Directory as described in Chapter 9.

6. Provision the Oracle Identity Management users as described in Section 11.4.3, "Creating Users and Groups for Oracle Identity Manager."

7. On `IDMHOST1`, edit the file *DOMAIN_HOME*`/config/fmwconfig/jps-config.xml`. Locate the entry that looks like this:

   ```
   <serviceInstance
   location=Path_to_Domain/config/fmwconfig/default-keystore.jks"
   provider="keystore.provider" name="keystore.ldap">
   ```

   Remove the Path from the keystore location so that the final entry looks like this:

   ```
   <serviceInstance location="./default-keystore.jks" provider="keystore.provider"
   name="keystore.ldap">
   ```

Save the file.

8. Stop all the managed servers running in your domain before extending the domain with Oracle Identity Manager.

> **Note:** Oracle SOA deployed along with Oracle Identity Manager is used exclusively for Oracle Identity Manager work flow. It cannot be used for other purposes.

13.2 Enabling Virtual IP Addresses on OIMHOST1 and OIMHOST2

The Identity Management domain uses virtual host names as the listen addresses for the Oracle Identity Manager and SOA managed servers. You must enable two virtual IP addresses mapping each of these host names on each of the two Oracle Identity Manager machines. Specifically, enable `OIMVHN1` and `SOAVHN1` on `OIMHOST1` and enable `OIMVHN2` and `SOAVHN2` on `OIMHOST2`. These virtual addresses must correctly resolve to the virtual host names in the network system used by the topology, either by DNS Server or by hosts resolution.

To enable the virtual IP addresses, follow the steps described in Section 6.1, "Enabling ADMINVHN on IDMHOST1." These virtual IP addresses and virtual host names are required to enable server migration for the Oracle Identity Manager and SOA servers. Server migration must be configured for the Oracle Identity Manager and SOA managed servers for high availability purposes.

> **See Also:** Chapter 16, "Configuring Server Migration for Oracle Identity Manager" for more details about configuring server migration for the Oracle Identity Manager and SOA Managed servers.

13.3 Extending the Domain to Configure Oracle Identity Manager and Oracle SOA Suite on IDMHOST1

Although you deploy Oracle Identity Manager on servers dedicated to it (`OIMHOST1` and `OIMHOST2`), you must first extend the WebLogic domain with Oracle Identity Manager on `IDMHOST1`. Configure Oracle Identity Manager on IDMHOST1 as follows.

To extend the domain with Oracle Identity Manager on `IDMHOST1`, start the configuration wizard by executing the command:

`ORACLE_COMMON_HOME/common/bin/config.sh`

Proceed as follows

1. On the Welcome screen, select **Extend an existing WebLogic Domain**.

   Click **Next**.

2. On the Select WebLogic Domain Directory screen, select the location of the domain directory for the OIM domain. For Example:
   `/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain`.

   Click **Next**.

3. On the Select Extension Source screen, select **Extend my domain automatically to support the following added products**. From the list below, select: **Oracle Identity Manager**.

> **Note:** **Oracle SOA Suite** and **Oracle WSM Policy Manager** are selected automatically. If Oracle WSM Policy Manager has already been installed, the choice is not available.

Select **Next**.

4. The Configure RAC Multi Data Sources screen displays the schedulerDS Data Source configured for Oracle Directory Integration Platform and Oracle Directory Services manager (ODSM). Do not make any selections or changes on this screen.

   Click **Next**.

5. On the Configure JDBC Component Schemas screen, select all the data sources listed on the page:

   - **SOA Infrastructure**
   - **User Messaging Service**
   - **OIM MDS Schema**
   - **OWSM MDS Schema**
   - **SOA MDS Schema**
   - **OIM Schema**

   Select **Configure selected component schemas as RAC multi data source schemas** in the next panel.

   Click **Next**.

6. On the Configure RAC Multi Data Source Component Schema page, select all the schemas for your component. Do not select schemas listed for previously configured components. Then enter the following information:

Schema Name	Service Name	Host Names	Instance Names	Port	Schema Owner	Password
SOA Infrastructure	oimedg.mycompany.com	idmdbhost1-vip.mycompany.com	oimedg1	1521	EDG_SOAINFRA	*password*
		idmdbhost2-vip.mycompany.com	oimedg2	1521		
User Messaging Service	oimedg.mycompany.com	idmdbhost1-vip.mycompany.com	oimedg1	1521	EDG_ORASDPM	*password*
		idmdbhost2-vip.mycompany.com	oimedg2	1521		
OIM MDS Schema	oimedg.mycompany.com	idmdbhost1-vip.mycompany.com	oimedg1	1521	EDG_MDS	*password*
		idmdbhost2-vip.mycompany.com	oimedg2	1521		
OWSM MDS Schema	oidedg.mycompany.com	oiddbhost1-vip.mycompany.com	idmedg1	1521	EDG_MDS	*password*

Schema Name	Service Name	Host Names	Instance Names	Port	Schema Owner	Password
		oiddbhost2-vip.mycompany.com	idmedg2	1521		
SOA MDS Schema	oimedg.mycompany.com	idmdbhost1-vip.mycompany.com	oimedg1	1521	EDG_MDS	*password*
		idmdbhost2-vip.mycompany.com	oimedg2	1521		
OIM Schema	oimedg.mycompany.com	idmdbhost1-vip.mycompany.com	oimedg1	1521	EDG_OIM	*password*
		idmdbhost2-vip.mycompany.com	oimedg2	1521		

If you are using Oracle Database 11.2, replace the `vip` addresses with the 11.2 SCAN address.

Click **Next**.

7. On the Test Component Schema screen, the Configuration Wizard attempts to validate the data sources. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the problem, and try again.

   Click **Next**.

8. On the Select Optional Configuration screen, Select:

   - **JMS Distributed Destination**
   - **Managed Servers, Clusters and Machines**
   - **JMS File Store**

   Click **Next**.

9. On the JMS Distributed Destination screen, ensure that all the JMS system resources listed on the screen are uniform distributed destinations. If they are not, select **UDD** form the drop down box. Ensure that the entries look like this:

JMS System Resource	Uniform/Weighted Distributed Destination
UMSJMSSystemResource	UDD
SOAJMSModule	UDD
OIMJMSModule	UDD
BPMJMSModule	UDD

Click **Next**.

An Override Warning box with the following message is displayed:

```
CFGFWK-40915: At least one JMS system resource has been selected for conversion
to a Uniform Distributed Destination (UDD). This  conversion will take place
only if the JMS System resource is assigned to a cluster
```

Click **OK** on the Override Warning box.

10. When you first enter the Configure Managed Servers screen, two managed servers called `oim_server1` and `soa_server1` are created automatically. Rename `soa_server1` to `WLS_SOA1` and `oim_server1` to `WLS_OIM1` and update their attributes as shown in the following table. Then, add two new managed servers called `WLS_OIM2` and `WLS_SOA2` with the following attributes.

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_SOA1	SOAVHN1	8001	N/A	No
WLS_OIM1	OIMVHN1	14000	N/A	No
WLS_OIM2	OIMVHN2	14000	N/A	No
WLS_SOA2	SOAVHN2	8001	N/A	No

Notes:

- Do not change the configuration of the managed servers that were configured as a part of previous deployments.

- Do not delete the default managed servers that are created. Rename them as described.

11. On the Configure Clusters screen, create two clusters, by clicking **Add**. Supply the following information:

OIM Cluster:

- **Name**: `cluster_oim`

- **Cluster Messaging Mode**: `unicast`

SOA Cluster:·

- **Name**: `cluster_soa`

- **Cluster Messaging Mode**: `unicast`

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

Note: Do not change the configuration of the clusters that were configured as a part of previous deployments.

12. 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.

The **cluster_oim** has the managed servers **WLS_OIM1** and **WLS_OIM2** as members.

The **cluster_soa** has the managed servers **WLS_SOA1** and **WLS_SOA2** as members.

Click **Next**.

> **Note:** Do not make any changes to clusters that already have entries defined.

13. On the Configure Machines screen, create a machine for each host in the topology.

    a. Click the tab **UNIX** if your hosts use Linux or a UNIX-based operating system. Otherwise, click **Machines**.

    b. **Name**: Name of the host. Best practice is to use the DNS name.

    c. **Node Manager Listen Address**: DNS name of the machine.

    d. **Node Manager Port**: Port for Node Manager

    Provide the information shown in the following table.

Name	Node Manager Listen Address	Node Manager Listen Port
OIMHOST1	OIMHOST1	5556
OIMHOST2	OIMHOST2	5556

    Leave the default values for all other fields.

    Delete the default local machine entry under the **Machines** tab.

    Click **Next**.

14. On the Assign Servers to Machines screen, indicate which managed servers to run on each of the machines you created.

    Click a machine in the right pane.

    Click the managed servers you want to run on that machine in the left pane.

    Click the arrow to assign the managed servers to the machines.

    Repeat until all managed servers are assigned to machines.

    For example:

    - **OIMHOST1**: `WLS_OIM1` and `WLS_SOA1`

    - **OIMHOST2**: `WLS_OIM2` and `WLS_SOA2`

    Click **Next** to continue.

15. On the Configure JMS File Stores screen, update the directory locations for the JMS file stores. Provide the information shown in the following table.

Name	Directory
UMSJMSFileStore_ auto_1	`/u01/app/oracle/admin/`*IDMDomain*`/soa_ cluster/jms/UMSJMSFileStore_auto_1`
UMSJMSFileStore_ auto_2	`/u01/app/oracle/admin/`*IDMDomain*`/soa_ cluster/jms/UMSJMSFileStore_auto_2`
BPMJMSServer_auto_1	`/u01/app/oracle/admin/`*IDMDomain*`/soa_ cluster/jms/BPMJMSServer_auto_1`
BPMJMSServer_auto_2	`/u01/app/oracle/admin/`*IDMDomain*`/soa_ cluster/jms/BPMJMSServer_auto_2`

Name	Directory
SOAJMSFileStore_auto_1	/u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/SOAJMSFileStore_auto_1
SOAJMSFileStore_auto_2	/u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/SOAJMSFileStore_auto_2
OIMJMSFileStore_auto_1	/u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/OIMJMSFileStore_auto_1
OIMJMSFileStore_auto_2	/u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/OIMJMSFileStore_auto_2

Click **Next**.

> **Notes:**
>
> - Use /u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/ as the directory location for the UMSJMSFileStore_auto_1, UMSJMSFileStore_auto_2, BPMJMSServer_auto_1, BPMJMSServer_auto_2, SOAJMSFileStore_auto_1, and SOAJMSFileStore_auto_2 JMS file stores
>
> - Use /u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/ as the directory location for the OIMJMSFileStore_auto_1 and OIMJMSFileStore_auto_2 JMS file stores
>
> - The locations /u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/ and /u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/ are on shared storage and must be accessible from OIMHOST1 and OIMHOST2

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

17. On the Installation Complete screen, click **Done**.

18. Restart WebLogic Administration Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.4 Configuring Oracle Identity Manager on IDMHOST1

You must configure the Oracle Identity Manager server instances before you can start the Oracle Identity Manager and SOA Managed Servers. The Oracle Identity Management Configuration Wizard loads the Oracle Identity Manager metadata into the database and configures the instance.

Before proceeding, ensure that the following are true:

- The Administration Server is up and running.

- The environment variables DOMAIN_HOME and WL_HOME are *not* set in the current shell.

The Oracle Identity Management Configuration Wizard is located under the Identity Management Oracle home. Type:

IAM_ORACLE_HOME/bin/config.sh

Proceed as follows:

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

2. On the Components to Configure screen, Select **OIM Server**.

> **Note:** Oracle Identity Manager Remote Manager is optional in Fusion Applications implementations

   Click **Next**.

3. On the Database screen, provide the following values:

   - **Connect String**: The connect string for the Oracle Identity Manager database:

     `oimdb1-vip.mycompany.com:1521:oimedg1^oimdb2-vip.mycompany`
     `.com:1521:oimedg2@oimedg.mycompany.com`

   - **OIM Schema User Name**: `edg_oim`

   - **OIM Schema password**: *password*

   - **MDS Schema User Name**: `edg_mds`

   - **MDS Schema Password**: *password*

   Select **Next**.

4. On the WebLogic Administration Server screen, provide the following details for the WebLogic Administration Server:

   - **URL**: The URL to connect to the WebLogic Administration Server. For example: `t3://adminvhn.mycompany.com:7001`

   - **UserName**: `weblogic`

   - **Password**: Password for the `weblogic` user

   Click **Next**.

5. On the OIM Server screen, provide the following values:

   - **OIM Administrator Password**: Password for the Oracle Identity Manager Administrator. This is the password for the `xelsysadm` user. The password must contain an uppercase letter and a number.

   - **Confirm Password**: Confirm the password·

   - **OIM HTTP URL**: Proxy URL for the Oracle Identity Manager Server. This is the URL for the Hardware load balancer that is front ending the OHS servers for Oracle Identity Manager. For example: `http://oiminternal.mycompany.com:80.`

   - **Key Store Password**: Key store password. The password must have an uppercase letter and a number. Best practice is to use the same password that you assigned to the user `xelsysadm` in Section 11.4.3, "Creating Users and Groups for Oracle Identity Manager."

   Click **Next**.

6. On the BI Publisher screen, provide the following values:

   - **Configure BI Publisher**: Select if you want to Configure Oracle Identity Manager with Oracle BI Publisher. This is Optional and depends on your requirements.

- **BI Publisher URL**: The URL of BI Publisher, if you selected it.

- **Enable LDAP Sync**: Selected.

> **Notes:** BI Publisher is not a part of the *IDMDomain*. The steps to configure the BI Publisher are not covered in this Enterprise Deployment Guide.

Click **Next**.

7. On the LDAP Server Screen, the information you enter is dependent on your implementation. Provide the following details:

   - **Directory Server Type**:

     - `OID`, if your Identity Store is in `OID`.

     - `OVD` if you access your Identity Store through `OVD`.

   - **Directory Server ID**: A name for your Oracle Internet Directory server. For example: `IdStore`. This is only required if the directory type is `OID`.

   - **Server URL**: The LDAP server URL. For example: `ldap://idstore.mycompany.com:389`

   - **Server User**: The user name for connecting to the LDAP Server. For example: `cn=oimadmin,cn=systemids,dc=mycompany,dc=com`

   - **Server Password**: The password for connecting to the LDAP Server.

   - **Server Search DN**: The Search DN, if you are accessing your IDStore using Oracle Virtual Directory Server. For example: `dc=mycompany,dc=com`.

   Click **Next**.

8. On the LDAP Server Continued screen, provide the following LDAP server details:

   - **LDAP Role Container**: The DN for the Role Container. This is the container where the Oracle Identity Manager roles are stored. For example: `cn=Groups,dc=mycompany,dc=com`·

   - **LDAP User Container**: The DN for the User Container. This is the container where the Oracle Identity Manager users are stored. For example: `cn=Users,dc=mycompany,dc=com`·

   - **User Reservation Container**: The DN for the User Reservation Container. For example: `cn=Reserve,dc=mycompany,dc=com`.

   Click **Next**.

9. On the Configuration Summary screen, verify the summary information.

   Click **Configure** to configure the Oracle Identity Manager instance

10. On the Configuration Progress screen, once the configuration completes successfully, click **Next**.

11. On the Configuration Complete screen, view the details of the Oracle Identity Manager Instance configured.

    Click **Finish** to exit the Configuration Assistant.

12. Restart WebLogic Administration Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.5 Propagating the Oracle Identity Manager and SOA Managed Servers to Oracle Identity Manager Servers

Once the configuration has succeeded on IDMHOST1, you can propagate the configuration to `OIMHOST1` and `OIMHOST2` (Enterprise deployment only). You do this by packing the domain on `IDMHOST1` and unpacking it on `OIMHOST1` and `OIMHOST2` (Enterprise deployment only).

Follow these steps to propagate the domain to `IDMHOST1`.

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

   ```
   ./pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
   -template=/u01/app/oracle/admin/templates/oim_domain.jar -template_name="OIM
   Domain" -managed=true
   ```

2. This creates a file called `oim_domain.jar` in the `/u01/app/oracle/admin/templates` directory. Copy this file to `OIMHOST1` and `OIMHOST2`.

3. On `OIMHOST1`, invoke the utility `unpack`, which is also located in the directory `ORACLE_COMMON_HOME/common/bin/`.

   ```
   ./unpack.sh -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain
   -template=/u01/app/oracle/product/fmw/templates/oim_domain.jar -overwrite_
   domain=true -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
   ```

4. On `OIMHOST2`, invoke the utility `unpack`, which is also located in the directory `ORACLE_COMMON_HOME/common/bin/`.

   ```
   ./unpack.sh -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain
   -template=/u01/app/oracle/product/fmw/templates/oim_domain.jar -overwrite_
   domain=true -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
   ```

5. Copy the `soa` directory located under the `/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain` directory on `IDMHOST1` to the `/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain` directory on `OIMHOST1` and `OIMHOST2`.

   To copy the `soa` directory from `IDMHOST1` to `OIMHOST1`:

   ```
   scp -rp /u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/soa
   user@OIMHOST1:/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain/soa
   ```

   To Copy the soa directory from `IDMHOST1` to `OIMHOST2`:

   ```
   scp -rp /u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/soa
   user@OIMHOST2:/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain/soa
   ```

6. Copy the `setDomainEnv.sh` and the `setSOADomainEnv.sh` under the

   `/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain/bin` directory on `oimhost1`

   to the `/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain/bin` directory on IDMHOST1 and IDMHOST2.

7. Start the Managed Servers in your domain, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," except for the following servers:

   - WLS_OIM1

- WLS_OIM2

- WLS_SOA1

- WLS_SOA2

13.6 Post-Installation Steps on OIMHOST1

This section describes post-installation steps.

This section contains the following topics:

- Section 13.6.1, "Updating the Coherence Configuration for the SOA Managed Server"

- Section 13.6.2, "Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1"

- Section 13.6.3, "Validating Oracle Identity Manager Instance on OIMHOST1"

13.6.1 Updating the Coherence Configuration for the SOA Managed Server

Follow these steps to update the Coherence Configuration for the `WLS_SOA` Server.

1. Log in to the Oracle WebLogic Server Administration Console.

2. Click **Lock and Edit**.

3. In the Domain Structure window, expand the **Environment** node.

4. Click **Servers**. The Summary of Servers page appears.

5. Click the name of the server in the Name (`WLS_SOA1`/`WLS_SOA2`) column of the table. The settings page for the selected server appears.

6. Click the **Server Start** tab.

7. Enter text into the Arguments field for `WLS_SOA1` and `WLS_SOA2`.

   For `WLS_SOA1`, enter the following text on a single line, without a carriage return:

   ```
   -Dtangosol.coherence.wka1=soavhn1 -Dtangosol.coherence.wka2=soavhn2
   -Dtangosol.coherence.localhost=soavhn1
   ```

   For `WLS_SOA2`, enter the following text on a single line, without a carriage return:

   ```
   -Dtangosol.coherence.wka1=soavhn1 -Dtangosol.coherence.wka2=soavhn2
   -Dtangosol.coherence.localhost=soavhn2
   ```

> **Note:** The Coherence cluster used for deployment uses port 8088 by
> default. You can change this port by specifying a different port (for
> example, `8089`) with the `-Dtangosol.coherence.wkan.port`
> and `-Dtangosol.coherence.localport` startup parameters. For
> example:
>
> For WLS_SOA1 (on a single line):
>
> ```
> -Dtangosol.coherence.wka1=soavhn1 -Dtangosol.coherence.wka2=soavhn2
> -Dtangosol.coherence.localhost=soavhn1
> -Dtangosol.coherence.localport=8089
> -Dtangosol.coherence.wka1.port=8089
> -Dtangosol.coherence.wka2.port=8089
> ```
>
> For WLS_SOA2 (on a single line):
>
> ```
> -Dtangosol.coherence.wka1=soavhn1 -Dtangosol.coherence.wka2=soavhn2
> -Dtangosol.coherence.localhost=soavhn2
> -Dtangosol.coherence.localport=8089
> -Dtangosol.coherence.wka1.port=8089
> -Dtangosol.coherence.wka2.port=8089
> ```

8. Click **Save** and activate the changes.

> **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.
>
> Do not copy the text from this section to your Administration
> Console's arguments text field. Doing so can cause HTML tags to be
> inserted in the Java arguments. The text should not include any text or
> characters other than the ones shown.

13.6.2 Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1

Follow this sequence of steps to start the `WLS_OIM1` and `WLS_SOA1` Managed Servers
on `OIMHOST1`:

1. Stop the WebLogic Administration Server on `IDMHOST1` by using the WebLogic
   Administration Console as described in Section 19.1, "Starting and Stopping
   Oracle Identity Management Components."

2. Start the Administration Server on `IDMHOST1` using the Node Manager, as
   described in Section 19.1, "Starting and Stopping Oracle Identity Management
   Components."

3. Validate that the Administration Server started up successfully by bringing up the
   Oracle WebLogic Administration Console.

4. Start NodeManager on `OIMHOST1`. Create the `nodemanager.properties` file
   by using the `startNodemanager.sh` script located under the *MW_*
   HOME`/wlserver_10.3/server/bin` directory.

5. Before you can start the Managed Servers by using the console, node manager
   requires that the property `StartScriptEnabled` be set to `true`. You set it by

running the `setNMProps.sh` script located under the *MW_HOME*/`oracle_common/common/bin` directory.

```
prompt> MW_HOME/oracle_common/common/bin/setNMProps.sh
```

6. Restart the Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components" so that the properties take effect.

7. Start the `WLS_SOA1` Managed Server, using the WebLogic Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

8. Start the `WLS_OIM1` Managed Server using the WebLogic Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.6.3 Validating Oracle Identity Manager Instance on OIMHOST1

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

```
http://oimvhn1.mycompany.com:14000/oim
```

Log in using the `xelsysadm` username and password.

> **Note:** When you log in for the first time, you are prompted to setup Challenge Questions. Please do so before proceeding further.

Validate Oracle SOA Suite using the URL:

```
http://oimvhn1.mycompany.com:8001/soa-infra
```

Log in as the `weblogic` user.

13.7 Post-Installation Steps on OIMHOST2

It describes the post-installation steps on `OIMHOST2`.

This section contains the following topics:

- Section 13.7.1, "Starting Node Manager on OIMHOST2"
- Section 13.7.2, "Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2"
- Section 13.7.3, "Validating Oracle Identity Manager Instance on OIMHOST2"

13.7.1 Starting Node Manager on OIMHOST2

1. Start the Node Manager on `OIMHOST2` to create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the *MW_HOME*/`wlserver_10.3/server/bin` directory.

2. Before you can start the Managed Servers by using the console, node manager requires that the property `StartScriptEnabled` is set to true. You set it by running the `setNMProps.sh` script located under the *MW_HOME*/`oracle_common/common/bin` directory.

```
prompt>  MW_HOME/oracle_common/common/bin
prompt> ./setNMProps.sh
```

3. Restart the Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components" so that the properties take effect.

13.7.2 Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2

Follow this sequence of steps to start the `WLS_OIM2` Managed Server on `OIMHOST2`:

1. Start the `WLS_SOA2` Managed Server, using the WebLogic Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

2. Start the `WLS_OIM2` Managed Server using the WebLogic Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.7.3 Validating Oracle Identity Manager Instance on OIMHOST2

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

`http://oimvhn2.mycompany.com:14000/oim/`

Log in using the `xelsysadm` username and password

Validate SOA at:

`http://oimvhn2.mycompany.com:8001/soa-infra`

Log in as the `weblogic` user.

13.8 Modifying the Oracle Identity Manager Default System Properties for UserName Generation

When first installed, Oracle Identity Manager has a set of default system properties for its operation.

If your Identity Store is in Active Directory, you must change the System property `XL.DefaultUserNamePolicyImpl` to `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD` or `oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstNamePolicyForAD`.

To learn how to do this, see the Administering System Properties chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

13.9 Configuring Oracle Identity Manager to Reconcile from ID Store

In the current release, the `LDAPConfigPostSetup` script enables all the LDAPSync-related incremental Reconciliation Scheduler jobs, which are disabled by default. The LDAP configuration post-setup script is located under the *IAM_ORACLE_HOME*/server/ldap_config_util directory. Run the Script on IDMHOST1, as follows:

1. Edit the `ldapconfig.props` file located under the *IAM_ORACLE_HOME*/server/ldap_config_util directory and provide the following values:

Parameter	Value	Description
`OIMAdminUser`	`xelsysadm`	Oracle Identity Manager system administrator
`OIMProviderURL`	`t3://oimvhn1.mycompany.com:14000,oimvhn2.mycompany.com:14000`	List of Oracle Identity Manager managed servers.
`OIDURL`	Specify the URL for the Oracle Internet Directory instance, for example: `ldap://localhost:389`[1]	Identity Store URL.
`OIDAdminUsername`	`cn=oimadmin,cn=systemids,dc=mycompany,dc=com`	Name of use used to connect to Identity Store. This user should **not** be located in `cn=Users,dc=mycompany,dc=com`.
`OIDSearchBase`	`dc=mycompany,dc=com`	Root location in Identity Store where Users and Groups are located.
`UserContainerName`	`cn=Users`	cn of User location within Search base.
`RoleContainerName`	`cn=Groups`	cn of Groups location within Search base.
`ReservationContainerName`	`cn=Reserve`	cn of Reserve location within Search base.

[1] If you are usingActive Directory or Oracle Virtual Directory as the directory server, specify the appropriate URL

Note: `usercontainerName`, `rolecontainername`, and `reservationcontainername` are not used in this step.

---

2. Save the file.

3. Set the `JAVA_HOME` and `WL_HOME` environment variables.

4. Run LDAPConfigPostSetup.sh. The script prompts for the Oracle Internet Directory admin password and the Oracle Identity Manager admin password. For example:

```
Prompt> ./LDAPConfigPostSetup.sh
[Enter OID admin password: ]
[Enter OIM admin password: ]
```

13.10 Configuring Oracle Identity Manager to Work with the Oracle Web Tier

This section describes how to configure Oracle Identity Manager to work with the Oracle Web Tier.

This section contains the following topics:

- Section 13.10.1, "Prerequisites"

- Section 13.10.2, "Configuring Oracle HTTP Servers to Front End the Oracle Identity Manager & SOA Managed Servers"

- Section 13.10.3, "Changing Host Assertion in WebLogic"

- Section 13.10.4, "Validating Oracle Identity Manager Instance from the WebTier"

13.10.1 Prerequisites

Before configuring Oracle Identity Manager to work with the Oracle Web Tier, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on `WEBHOST1` and `WEBHOST2`.

2. Install and configure Oracle Identity Manager on `IDMHOST1` and `IDMHOST2`.

3. Configure the load balancer with a virtual host name (`sso.mycompany.com`) pointing to the web servers on `WEBHOST1` and `WEBHOST2`.

4. Configure the load balancer with a virtual host name (`admin.mycompany.com`) pointing to web servers `WEBHOST1` and `WEBHOST2`.

13.10.2 Configuring Oracle HTTP Servers to Front End the Oracle Identity Manager & SOA Managed Servers

1. On each of the web servers on `WEBHOST1` and `WEBHOST2`, create a file called `oim.conf` in the directory *ORACLE_INSTANCE*`/config/OHS/component/moduleconf`.

   This file must contain the following information:

```
# oim admin console(idmshell based)
  <Location /admin>
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   WLCookieName     oimjsessionid
   WebLogicCluster oimvhn1:14000,oimvhn2:14000
   WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

# oim self and advanced admin webapp consoles(canonic webapp)

  <Location /oim>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName     oimjsessionid
    WebLogicCluster oimvhn1:14000,oimvhn2:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
  <Location /sodcheck>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName     oimjsessionid
    WebLogicCluster soavhn1:8001,soavhn2:8001
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
```

```
              # Callback webservice for SOA. SOA calls this when a request is
          approved/rejected
          # Provide the SOA Managed Server Port
            <Location /workflowservice>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>

          # xlWebApp - Legacy 9.x webapp (struts based)
             <Location /xlWebApp>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>

          # Nexaweb WebApp - used for workflow designer and DM
            <Location /Nexaweb>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>

          # used for FA Callback service.
            <Location /callbackResponseService>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>

          # spml xsd profile
            <Location /spml-xsd>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>

            <Location /HTTPClnt>
              SetHandler weblogic-handler
              WLProxySSL ON
              WLProxySSLPassThrough ON
              WLCookieName    oimjsessionid
              WebLogicCluster oimvhn1:14000,oimvhn2:14000
              WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
            </Location>
```

2. Save the file on both `WEBHOST1` and `WEBHOST2`.

3. Stop and start the Oracle HTTP Server instances on both `WEBHOST1` and `WEBHOST2` as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.10.3 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 at `http://admin.mycompany.com/console`. 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** (**cluster_soa**).

4. In the **General** tab, select the **HTTP** subtab.

   Enter:

   - **Frontend Host**: `sso.mycompany.com`

   - **Frontend HTTPS Port**: `443`

5. Click **Save**.

6. Click **Activate Changes** in the Change Center window to enable editing.

7. Restart `WLS_OIM1` and `WLS_OIM2` as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

13.10.4 Validating Oracle Identity Manager Instance from the WebTier

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

`https://sso.mycompany.com:443/oim`

Log in using the `xelsysadm` username and password.

> **Note:** If you have installed Oracle Access Manager 11*g*, you might have to log in twice, first as an Oracle Access Manager user and then as the `xelsysadm` user at the OIM login page. This is resolved when you integrate Oracle Identity Manager with Oracle Access Manager 11g.

13.11 Configuring a Default Persistence Store for Transaction Recovery

The `WLS_OIM` and `WLS_SOA` Managed Servers have a transaction log that stores information about committed transactions that are coordinated by the server that might not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability

of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

> **Note:** Preferably, this location should be on a dual-ported SCSI disk or on a Storage Area Network (SAN).

Perform these steps to set the location for the default persistence stores for the Oracle Identity Manager and SOA Servers:

1. Create the following directories on the shared storage:

   ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs

   ORACLE_BASE/admin/domain_name/oim_cluster_name/tlogs

2. Log in to the Oracle WebLogic Server Administration Console.

3. Click **Lock and Edit**.

4. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.

   The Summary of Servers page is displayed.

5. Click the name of either the Oracle Identity Manager or the SOA server (represented as a hyperlink) in the **Name** column of the table.

6. The Settings page for the selected server is displayed, and defaults to the **Configuration** tab.

7. Open the **Services** sub tab.

8. Under the **Default Store** section of the page, provide the path to the default persistent store on shared storage. The directory structure of the path is as follows:

   - For Oracle Identity Manager Servers: *ORACLE_BASE*/admin/domain_name/oim_cluster_name/tlogs

   - For SOA Servers: *ORACLE_BASE*/admin/domain_name/soa_cluster_name/tlogs

   > **Note:** To enable migration of the Transaction Recovery Service, specify a location on a persistent storage solution that is available to other servers in the cluster. All the servers that are a part of the cluster must be able to access this directory.

9. Click **Save and Activate**.

10. Restart the Oracle Identity Manager and SOA Managed Servers, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," to make the changes take effect.

13.12 Configuring an IT Resource Instance for Email

This section describes how to set up email notification. This is mandatory for Fusion Applications. The following steps assume that an email server has been set up and that Oracle Identity Management can use it to send the email notifications.

1. Log in to Oracle Identity Manager Advanced Administration as system administrator.

2. Navigate to **Configuration -> Create IT Resource**.

3. Enter `Email Server` for **IT Resource Name**. Select **Mail Server** for **IT Resource Type**. Do not select anything for the **Remote Manager** field. Click **Continue**.

4. On the **Step 2: Specify IT Resource Parameter Values** page, provide the following values for the fields:

   - **Authentication**: `False`

   - **Server Name**: *Email server name*, for example: `mail.mycompany.com`

     User Login: leave blank

   - **User Password**: leave blank

   Click **Continue**.

5. On the **Step 3: Set Access Permission to IT Resource** page, do not change anything. Click **Continue**.

6. On the **Step 4: Verify IT Resource Details** page, check all the values you entered to verify that they are correct. Click **Continue**.

7. On the **Step 5: IT Resource Connection Result** page, Oracle Identity Manager checks whether it can connect to the email server provided. If the connection is successful, click **Create**.

8. On the **Step 6: IT Resource Created** page, click **Finish**.

9. Restart the Oracle Identity Manager server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," for the changes to take effect.

13.13 Enabling OIM to Connect to SOA Using the Administrative Users Provisioned in LDAP

Oracle Identity Manager connects to SOA as SOA administrator, with the username `weblogic` by default. As mentioned in the previous sections, a new administrator user is provisioned in the central LDAP store to manage Identity Management Weblogic Domain.

Perform the following postinstallation steps to enable Oracle Identity Manager to work with the Oracle WebLogic Server administrator user provisioned in the central LDAP store. This enables Oracle Identity Manager to connect to SOA without any problem:

1. Log in to Enterprise Manager at: `http://admin.mycompany.com/em`

2. Right click **Identity and Access/oim(11.1.1.3.0)** and select **System Mbean Browser**.

3. Expand **oracle.iam** under **application-defined Mbeans**, and select **Server**: **OIM_SERVER_NAME**, **Application**: **oim**, **XML config**, **config**, **XMLConfig.SOAConfig**, and then select the **SOAConfig Mbean**.

4. View the **username** attribute. By default, the value of this attribute is `weblogic`. Change this to the Oracle WebLogic Server administrator username provisioned in Section 11.4.3, "Creating Users and Groups for Oracle Identity Manager," for example: `weblogic_idm`

5. Click **Apply**.

6. Navigate to the *IAM_ORACLE_HOME*/common/bin/ directory in the Oracle Identity Manager deployment.

7. Start the WebLogic Scripting Tool (WLST) by running the following command:

   ```
   ./wlst.sh
   ```

8. At the prompt, enter `connect()`. When prompted, enter the Oracle WebLogic Server administrator username, password, and administrative server connection string.

9. Delete the default SOA administrator username and password credential from CSF by running the following command:

   ```
   deleteCred(map="oim", key="SOAAdminPassword");
   ```

10. Create the new credential that Oracle Identity Manager uses to connect to SOA as SOA administrator by running the following command:

    ```
    createCred(map="oim", key="SOAAdminPassword", user="weblogic_
    idm",password="ADMINISTRATOR_PASSWORD");
    ```

    Replace *ADMINISTRATOR_PASSWORD* with the actual password.

11. Confirm that the correct value has been seeded by running the following command:

    ```
    listCred(map="oim", key="SOAAdminPassword");
    ```

12. Exit WLST shell by running the following command:

    ```
    exit()
    ```

13. Log in to Oracle Identity Manager Administrative and User Console using the administrator login credentials.

14. Run the reconciliation process to enable the Oracle WebLogic Server administrator, `weblogic_idm`, to be visible in the OIM Console. Follow these steps:

    a. Log in to Oracle Identity Manager at:
       `https://sso.mycompany.com:443/oim` as the user `xelsysadm`.

    b. Click **Advanced**.

    c. Click the **System Management** tab

    d. Click the arrow for the **Search Scheduler** to list all the schedulers.

    e. Select **LDAP User Create** and **Update Full Reconciliation**.

    f. Click **Run Now** to run the job.

    g. Go to the Administration page and perform a search to verify that the user is visible in the Oracle Identity Manager console.

15. Search for the Administrators role. Open the role details and click the **Members** tab.

16. Add the newly created user as member of this role.

17. Restart Oracle Identity Manager managed server.

13.14 Tuning Oracle Platform Security

After installing Oracle Identity Manager, you must tune OPSS as described in the "Oracle Fusion Middleware Security Performance Tuning" chapter in the *Oracle Fusion Middleware Performance and Tuning Guide*.

In particular, set the following values when deploying Oracle Identity Management for Fusion Applications:

Attribute	Value
-Djps.subject.cache.key	5
-Djps.subject.cache.ttl	600000

13.15 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 5.5, "Backing up the Web Tier Configuration."

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 6.15, "Backing Up the WebLogic Domain."

4. Back up the Oracle Internet Directory as described in Section 7.7, "Backing up the Oracle Internet Directory Configuration."

5. Back up the Oracle Virtual Directory as described in Section 9.10, "Backing Up the Oracle Virtual Directory Configuration."

For information about backing up the application tier configuration, see Section 19.4, "Performing Backups and Recoveries."

14

Extending the Domain with Oracle Identity Federation

Oracle Identity Federation is a self-contained, standalone federation server that enables single sign-on and authentication in a multiple-domain identity network and supports the broadest set of federation standards. This enables users to federate in heterogeneous environments and business associations, whether they have implemented other Oracle Identity Management products in their solution set or not.

It can be deployed as a multi-protocol hub acting as both an Identity Provider (IdP) and Service Provider (SP).

Acting as an SP, Oracle Identity Federation enables you to manage your resources while off loading actual authentication of users to an IdP, without having to synchronize users across security domains out of band. Once authenticated at the IdP, the SP can allow or deny access to users for the SP's applications depending upon the local access policies.

This chapter contains the following topics:

- Section 14.1, "Prerequisites"
- Section 14.2, "Configuring Oracle Identity Federation on OIFHOST1"
- Section 14.3, "Configuring Oracle Identity Federation on OIFHOST2"
- Section 14.4, "Provisioning the Managed Servers on the Local Disk"
- Section 14.5, "Validating Oracle Identity Federation"
- Section 14.6, "Configure the Enterprise Manager Agents"
- Section 14.7, "Enabling Oracle Identity Federation Integration with LDAP Servers"
- Section 14.8, "Configuring Oracle Identity Federation to work with the Oracle Web Tier"
- Section 14.9, "Validating Oracle Identity Federation"
- Section 14.10, "Backing Up the Application Tier Configuration"

14.1 Prerequisites

Before proceeding with Oracle Identity Federation configuration, ensure that you have done the following.

1. Install and upgrade the software on OIFHOST1 and OIFHOST2 as described in Section 4.5.3, "Installing Oracle WebLogic Server" and Section 4.5.4, "Installing Oracle Identity Management."

2. Run the Repository Creation Utility (RCU) to create and configure the collection of schemas used by Oracle Identity Federation as described in Chapter 3, "Configuring the Database Repositories."

3. Create the Identity Management domain as described in Chapter 6, "Creating the WebLogic Server Domain for Identity Management."

4. Install and configure Oracle Internet Directory as described in Chapter 7, "Extending the Domain with Oracle Internet Directory.".Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory is used as the User Store and the Federation Store

5. Install and configure Oracle HTTP Server on `WEBHOST1` and `WEBHOST2` as described in Chapter 5, "Configuring the Web Tier."

6. Associate the Identity Management domain created with an External LDAP Store as described in Section 11.3.2, "Reassociating the Policy and Credential Store." This is required because Oracle Identity Federation is being extended on a node where the Administration Server is not running.

14.2 Configuring Oracle Identity Federation on OIFHOST1

Ensure that the system, patch, kernel and other requirements are met. These are listed in the Oracle Fusion Middleware Installation Guide for Oracle Identity Management manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

On UNIX:

1. Ensure that port 7499 is 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.

   On UNIX:

   ```
   netstat -an | grep "7499"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   On UNIX:

   Remove the entries for port `7499` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

3. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

   ```
   #The port for OIF Server port
   OIF Server Port No = 7499
   ```

4. Start the Oracle Identity Management 11*g* Configuration Assistant located under the *IDM_ORACLE_HOME*/bin directory as follows:

On UNIX, issue this command:

```
./config.sh
```

On Windows, double-click `config.exe`

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

6. On the Select Domain screen, select Extend Existing Domain and specify these values:

   - **HostName**: `adminvhn.mycompany.com`

   - **Port**: `7001`

   - **UserName**: `weblogic`

   - **User Password**: *`weblogic_user_password`*

   Click **Next**.

7. A dialog box with the following message appears:

   ```
   The selected domain is not a valid Identity Management domain or the installer
   cannot determine if it is a valid domain. If you created the domain using the
   Identity Management installer, you can ignore this message and continue. If you
   did not create the domain using the Identity Management installer, refer to the
   Identity Management documentation for information on how to verify the domain
   is valid.
   ```

   This is a benign warning that you can ignore.

   Click **Yes** to continue.

8. On the Specify Installation Location screen, specify the following values:

   - **Oracle Middleware Home Location**: `/u01/app/oracle/product/fmw`

     This value is prefilled and cannot be updated.

   - **Oracle Home Directory**: `idm`

     This value is prefilled and cannot be updated

   - **WebLogic Server Directory**:
     `/u01/app/oracle/product/fmw/wlserver_10.3`

   - **Oracle Instance Location**: `/u01/app/oracle/admin/instances/oif_inst1`

   - **Instance Name**: `oif_inst1`

   Click **Next**.

9. On the Specify Oracle Configuration Manager Details screen, specify the values shown in this example:

   - **Email Address**: Provide the email address for your My Oracle Support account.

   - **Oracle Support Password**: Provide the password for your My Oracle Support account.

   - Select **I wish to receive security updates via My Oracle Support**.

   Click **Next**.

10. On the Configure Components screen, de-select all the components except Oracle Identity Federation components. Select only Oracle Identity Federation from the

Oracle Identity Federation components. Do not select Oracle HTTP Server. Select **Clustered**.

Click **Next**.

11. On the Configure Ports screen, select Specify Ports using Configuration File. Provide the path to the staticports.ini file that you copied to the temporary directory.

    Click **Next**.

12. On the Specify OIF Details screen, specify these values:

    ■ **PKCS12 Password**: *password*

    ■ **Confirm Password**: Confirm the password

    ■ **Server Id**: WLS_OIF1

    Click **Next**.

13. On the Select OIF Advanced Flow Attributes screen, specify these values:

    ■ **Authentication Type**: LDAP

    ■ **User Store**: LDAP

    ■ **Federation Store**: LDAP

    ■ **User Session Store**: RDBMS (default selection, which cannot be changed for a cluster)

    ■ **Message Store**: RDBMS (default selection, which cannot be changed for a cluster)

    ■ **Configuration Store**: RDBMS (default selection, which cannot be changed for a cluster)

    > **Note:** When you choose RDBMS for the session, message, and configuration data stores during an Advanced installation, the installer creates one data source for all three data stores. If you want to have separate databases for each of these stores, you must configure this after the installation by using the OUI Config Wizard.

    Click **Next**.

14. On the Authentication LDAP Details screen, specify the following values:

    ■ **LDAP Type**: Select **Oracle Internet Directory** from the drop down.

    ■ **LDAP URL**: The LDAP URL to connect to your LDAP store in the format: ldaps://host:port. For example: ldaps://oid.mycompany.com:636

    ■ **LDAP Bind DN**: cn=orcladmin

    ■ **LDAP Password**: *orcladmin_password*

    ■ **User Credential ID Attribute**: uid

    ■ **User Unique ID Attribute**: uid

    ■ **Person Object Class**: inetOrgPerson

    ■ **Base DN**: dc=mycompany,dc=com

    Click **Next**.

15. On the LDAP Attributes for User Data Store screen, specify the following values:

- **LDAP Type**: Select **Oracle Internet Directory** from the drop down.

- **LDAP URL**: The LDAP URL to connect to your LDAP store in the format: `ldaps://host:port`. For example: `ldaps://oid.mycompany.com:636`

- **LDAP Bind DN**: `cn=orcladmin`

- **LDAP Password**: *orcladmin_password*

- **User Description Attribute**: `uid`

- **User ID Attribute**: `uid`

- **Person Object Class**: `inetOrgPerson`

- **Base DN**: `dc=mycompany,dc=com`

Click **Next**.

16. On the LDAP Attributes for Federation Data Store screen, specify the following values:

- **LDAP Type**: Select **Oracle Internet Directory** from the drop down.

- **LDAP URL**: Provide the LDAP URL to connect to your LDAP store in the format: `ldaps://host:port`. For example: `ldaps://oid.mycompany.com:636`

- **LDAP Bind DN**: `cn=orcladmin`

- **LDAP Password**: *orcladmin_password*

- **User Federation Record Context**: `cn=myfed,dc=mycompany,dc=com`

- **Container Object Class**: The type of User Federation Record Context that Oracle Identity Federation should use when creating the LDAP container, if it does not exist already. If that field is empty, its value is set to `applicationprocess`. For Microsoft Active Directory this field must be set to `container`.

Click **Next**.

17. On the Transient Store Database Details screen, specify the values shown in this example:

- **Host Name**: The connect string to your database. For example:

  `oiddbhost1-vip.mycompany.com:1521:idmdb1^oiddbhost2-vip.mycompany.com:1521:idmdb2@oidedg.mycompany.com`

> **Notes:**
>
> - The Oracle RAC database connect string information must be provided in the format:
>
>   *host1*:*port1*:*instance1*^*host2*:*port2*:*instance2*@*servicename*
>
> - During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.
>
> - It is required that the information provided is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances.
>
>   Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.
>
> - If you are using Oracle Database 11.2, replace the `vip` addresses with the 11.2 SCAN address.

- - **UserName**: The username for the OIF Schema. For example: `edg_oif`

  - **Password**: *oif_user_password*

  Click **Next**.

18. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.

19. On the Configuration Progress screen, view the progress of the configuration.

20. On the Configuration Complete screen, click **Finish** to confirm your choice to exit.

14.3 Configuring Oracle Identity Federation on OIFHOST2

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. If you plan to provision the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in Section 2.4, "Shared Storage and Recommended Directory Structure."

3. Ensure that port `7499` is 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.

   On UNIX:

   ```
   netstat -an | grep "7499"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

On UNIX:

Remove the entries for port `7499` in the `/etc/services` file and restart the services, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," or restart the computer.

4. Copy the `staticports.ini` file from the Disk1/stage/Response directory to a temporary directory.

5. Edit the staticports.ini file that you copied to the temporary directory to assign the following custom port:

```
#The port for OIF Server port
OIF Server Port No = 7499
```

6. Start the Oracle Identity Management 11*g* Configuration Assistant located under the *IDM_ORACLE_HOME*/bin directory as follows:

   On UNIX, issue this command:

   ```
   ./config.sh
   ```

   On Windows, double-click `config.exe`

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

8. On the Select Domain screen, select the **Expand Cluster** option and specify these values:

   ■ **HostName**: `ADMINVHN.mycompany.com`

   ■ **Port**: `7001`

   ■ **UserName**: `weblogic`

   ■ **User Password**: *weblogic_user_password*

   Click **Next**.

9. A dialog box with the following message appears:

   ```
   The selected domain is not a valid Identity Management domain or the installer
   cannot determine if it is a valid domain. If you created the domain using the
   Identity Management installer, you can ignore this message and continue. If you
   did not create the domain using the Identity Management installer, refer to the
   Identity Management documentation for information on how to verify the domain
   is valid.
   ```

   This is a benign warning that you can ignore.

   Click **Yes** to continue.

10. On the Specify Installation Location screen, specify the following values:

    ■ **Oracle Middleware Home Location**: `/u01/app/oracle/product/fmw` (This value is prefilled and cannot be updated.)

    ■ **Oracle Home Directory**: `idm` (This value is prefilled and cannot be updated.)

    ■ **WebLogic Server Directory**: `/u01/app/oracle/product/fmw/wlserver_10.3`

    ■ **Oracle Instance Location**: `/u01/app/oracle/admin/instances/oif_inst2`

    ■ **Instance Name**: `oif_inst2`

    Click **Next**.

11. On the Specify Oracle Configuration Manager Details screen, specify the following 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**.

12. On the Configure Components screen, de-select all the components except for Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select **Oracle HTTP Server**.

    Click **Next**.

13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.

14. On the Configuration Progress screen, view the progress of the configuration.

15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

14.4 Provisioning the Managed Servers on the Local Disk

Due to certain limitations, the Oracle Configuration Wizard creates the domain configuration under the Identity Management Oracle home. In this deployment guide, the Oracle home is on shared disk and it is a best practice recommendation to separate the domain configuration from the Oracle home. This section provides the steps to separate the domain. Proceed as follows:

1. From `OIFHOST1`, copy the applications directory under the *MW_ HOME*/admin/*IDMDomain*/aserver/*IDMDomain*/config/fmwconfig/serve rs/wls_oif1 directory to the *MW_ HOME*/admin/*IDMDomain*/aserver/*IDMDomain*/config/fmwconfig/serve rs/wls_oif1 directory and to the *MW_ HOME*/admin/*IDMDomain*/aserver/*IDMDomain*/config/fmwconfig/serve rs/wls_oif2 directories on `IDMHOST1`.

   ```
   scp -rp MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_
   oif1/applications user@IDMHOST1:/ORACLE_
   BASE/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif1/
   scp -rp MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_
   oif1/applications user@IDMHOST1:/ORACLE_
   BASE/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif2/
   ```

2. On `IDMHOST1`, pack the Managed Server domain using the pack command located under the *ORACLE_COMMON_HOME*/common/bin directory. Make sure to pass the `-managed=true` flag to pack the Managed Server. Type:

   ```
   ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
      -domain=path_to_adminServer_domain -template=templateName.jar \
      -template_name=templateName
   ```

   For example

   ```
   ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
     -domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain \
     -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
     -template_name=ManagedServer_Template
   ```

3. Copy the Managed Server template directory from `IDMHOST1` to both `OIFHOST1` and `OIFHOST2`. For Example:

Copy to `OIFHOST1`:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@OIFHOST1:/u01/app/oracle/products/fmw/templates
```

Copy to `OIFHOST2`:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@OIFHOST2:/u01/app/oracle/products/fmw/templates
```

4. Unpack the Managed Server to the local disk on `OIFHOST1` using the `unpack` command located under the *ORACLE_COMMON_HOME*/`common/bin` directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
    -template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh \
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```

5. Unpack the Managed Server to the local disk on `OIFHOST2` using the `unpack` command located under the *ORACLE_COMMON_HOME*/`bin` directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk \
-overwrite_domain=true
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh \
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications \
-overwrite_domain=true
```

6. Run the `setNMProps.sh` command on both `OIFHOST1` and `OIFHOST2`.:

```
cd MW_HOME/oracle_common/common/bin
./setNMProps.sh
```

7. Restart the Node Manager on `OIFHOST1` and `OIFHOST2` by following the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

8. Restart the Administration server by following the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

9. Validate that the Administration Server started up successfully by opening a browser accessing the Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.

Also validate Enterprise Manager by opening a browser and accessing Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.

10. Restart the Managed Servers on `OIFHOST1` and `OIFHOST2` by using the Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

11. Delete the *MW_HOME*/admin/IDMDomain/aserver directory on OIFHOST1 and OIFHOST2. This directory is created by the Oracle Universal Installer when the domain is originally configured and is no longer required after the provisioning the Managed Server to the local disk.

14.5 Validating Oracle Identity Federation

Validate the configuration of Oracle Identity Federation on OIFHOST1 and OIFHOST2 by accessing the SP and IdP metadata on each host.

Proceed as follows on OIFHOST1:

1. Access the SP metadata by going to:

   `http://oifhost1.mycompany.com:7499/fed/sp/metadata`

2. Access the IdP metadata by going to:

   `http://oifhost1.mycompany.com:7499/fed/idp/metadata`

Proceed as follows on OIFHOST2:

1. Access the SP metadata by going to:

   `http://oifhost2.mycompany.com:7499/fed/sp/metadata`

2. Access the IdP metadata by going to:

   `http://oifhost2.mycompany.com:7499/fed/idp/metadata`

14.6 Configure the Enterprise Manager Agents

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage Oracle Identity Federation with this tool, you must configure the EM agents with the correct monitoring credentials. Update the credentials for the EM agents associated with OIFHOST1 and OIFHOST2. Follow these steps to complete this task:

1. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`. Log in as the WebLogic user.

2. From the Domain Home Page, navigate to the Agent-Monitored Targets page using the menu under **Farm -> Agent-Monitored Targets**.

   - Click the **Configure** link to go to the Configure Target Page.

   - On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.

   - Update the **WebLogic monitoring user name** and the **WebLogic monitoring password**. Enter weblogic as the WebLogic monitoring user name and the password for the weblogic user as the WebLogic monitoring password.

   - Click **OK** to save your changes.

14.7 Enabling Oracle Identity Federation Integration with LDAP Servers

By default, Oracle Identity Federation is not configured to be integrated with LDAP Servers deployed in a high availability configuration. To integrate Oracle Identity Federation with highly available LDAP Servers to serve as user data store, federation

data store, or authentication engine, you must configure Oracle Identity Federation based on the LDAP server's function.

Proceed as follows to integrate Oracle Identity Federation with an LDAP Server deployed in a high availability configuration

1. On `IDMHOST1`, set the `DOMAIN_HOME` environment variable to the Administration Server Domain home.

2. On `IDMHOST1`, set the environment using `the setOIFEnv.sh` script. This script is located under the `IDM_ORACLE_HOME`/fed/scripts directory.

   For example:

   ```
   IDMHOST1> export DOMAIN_HOME=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain
   IDMHOST1> cd IDM_ORACLE_HOME/fed/scripts
   IDMHOST1> . setOIFEnv.sh
   ```

3. On `IDMHOST1`, run the `WLST` script located under the `ORACLE_COMMON_HOME`/bin directory.

   ```
   IDMHOST1> cd ORACLE_COMMON_HOME/common/bin
   IDMHOST1> ./wlst.sh
   ```

4. Connect to one of the Oracle Identity Federation Managed Servers:

   ```
   wls:/offline> connect()
   ```

   Enter the username and password to connect to the Oracle Identity Federation Managed Servers. This is the same as the WebLogic Administration user name and password.

   Enter the URL to connect to the Oracle Identity Federation Managed Server:

   ```
   t3://OIFHOST1.mycompany.com:7499
   ```

5. Then enter the following properties, as needed:

   - To integrate the user data store with a highly available LDAP Server, set the `userldaphaenabled` boolean property from the `datastore` group to `true`:

     ```
     wls:/IDMDomain/serverConfig>
     setConfigProperty('datastore','userldaphaenabled', 'true', 'boolean')
     Update was successful for: userldaphaenabled
     ```

   - Validate the user data store is integrated with a highly available LDAP store by running:

     ```
     wls:/IDMDomain/serverConfig> getConfigProperty('datastore',
     'userldaphaenabled')
     Value(s) for property: true
     ```

     The userldaphaenabled property must return `true`.

   - To integrate the federation data store with a highly available LDAP Server, set the `fedldaphaenabled` boolean property from the `datastore` group to `true`:

     ```
     wls:/IDMDomain/serverConfig> setConfigProperty('datastore',
     'fedldaphaenabled','true', 'boolean')
     Update was successful for: fedldaphaenabled
     ```

   - Validate the federation data store is integrated with a highly available LDAP store by running:

```
wls:/IDMDomain/serverConfig> getConfigProperty('datastore',
'fedldaphaenabled')
Value(s) for property: true
```

The `fedldaphaenabled` property must return `true`.

- To integrate the LDAP authentication engine with a highly available LDAP Server, set the `ldaphaenabled` boolean property from the `authnengines` group to `true`:

```
wls:/IDMDomain/serverConfig>
setConfigProperty('authnengines','ldaphaenabled', 'true', 'boolean')
Update was successful for: ldaphaenabled
```

- Validate the LDAP authentication engine is integrated with a highly available LDAP store by running:

```
wls:/IDMDomain/serverConfig>
getConfigProperty('authnengines','ldaphaenabled')
Value(s) for property: true
```

The `ldaphaenabled` property for the `authnengines` group must return `true`.

Note: On `IDMHOST1`, delete the following directories:

- *ORACLE_ BASE*/admin/*IDMDomain*/aserver/*IDMDomain*/config/fmw config/servers/wls_oif1/applications

- *ORACLE_ BASE*/admin/*IDMDomain*/aserver/*IDMDomain*/config/fmw config/servers/wls_oif2/applications

---

14.8 Configuring Oracle Identity Federation to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier.

This section contains the following topics:

14.8.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Oracle Web Tier has been installed on WEBHOST1 and WEBHOST2.

2. Oracle Access Manager has been installed and configured on IDMHOST1 and IDMHOST2.

3. The load balancer has been configured with a virtual host name (sso.myconpany.com) pointing to the web servers on WEBHOST1 and WEBHOST2.

4. The load balancer has been configured with a virtual host name
(`admin.mycompany.com`) pointing to web servers WEBHOST1 and WEBHOST2.

14.8.2 Making Oracle Identity Federation aware of the Load Balancer

To configure the Oracle Identity Federation application to use the load balancer VIP,
follow these steps:

1. Log in to the Oracle Enterprise Manager Fusion Middleware Control console
using the credentials of the Administrative user (for example: `weblogic`).

2. Navigate to an OIF node in Oracle Enterprise Manager Fusion Middleware
Control. the OIF nodes are under **Identity and Access** in the navigation tree.

3. From the **OIF** menu, select **Administration**, and then Server **Properties**.

Change the host name to `sso.mycompany.com` and the port to `443`.

Select **SSL Enabled**.

Click **Apply**.

4. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control,
select **Administration**, and then **Identity Provider**.

Change the URL to `https://sso.mycompany.com:443/fed/idp`.

Click **Apply**.

5. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control,
select **Administration**, and then **Service Provider**.

Change the URL to `https://sso.mycompany.com:443/fed/sp`.

Click **Apply**.

14.8.3 Configuring Oracle HTTP Servers To Front End the Oracle Identity Federation Managed Servers

On each of the web servers on `WEBHOST1` and `WEBHOST2`, create a file called
`oif.conf` in the directory `ORACLE_`
`INSTANCE`/config/OHS/component/moduleconf. Edit this file and add the
following lines:

```
<Location /fed>
   SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
   WebLogicCluster oifhost1.mycompany.com:7499,oifhost2.mycompany.com:7499
</Location>
```

Restart the Oracle HTTP Server, as described in Section 19.1, "Starting and Stopping
Oracle Identity Management Components."

14.9 Validating Oracle Identity Federation

If the configuration is correct, you can access the following URLs from a web browser:

- `https://sso.mycompany.com/fed/sp/metadata`

- `https://sso.mycompany.com/fed/idp/metadata`

You should see metadata.

14.10 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 5.5, "Backing up the Web Tier Configuration."

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 application tier instances by following these steps:

    a. Shut down the instance using `opmnctl` located under the *ORACLE_INSTANCE*/`bin` directory:

        ORACLE_INSTANCE/bin/opmnctl stopall

    b. Create a backup of the Middleware home on the application tier. On Linux, as the `root` user, type:

        tar -cvpf *BACKUP_LOCATION*/apptier.tar *MW_HOME*

    c. Create a backup of the Instance home on the application tier as the `root` user:

        tar -cvpf *BACKUP_LOCATION*/instance_backup.tar *ORACLE_INSTANCE*

    d. Start up the instance using `opmnctl` located under the *ORACLE_INSTANCE*/`bin` directory:

        ORACLE_INSTANCE/bin/opmnctl startall

4. Back up the Administration Server domain directory as described in Section 6.15, "Backing Up the WebLogic Domain."

5. Back up the Oracle Internet Directory as described in Section 7.7, "Backing up the Oracle Internet Directory Configuration."

6. Back up the Oracle Virtual Directory as described in Section 9.10, "Backing Up the Oracle Virtual Directory Configuration."

15

Setting Up Node Manager

This chapter describes how to configure Node Manager in accordance with Oracle best practice recommendations. It contains the following sections:

- Section 15.1, "About Setting Up Node Manager"
- Section 15.2, "Changing the Location of the Node Manager Log"
- Section 15.3, "Enabling Host Name Verification Certificates for Node Manager"

15.1 About Setting Up Node Manager

Node Manager enables you to start and stop the Administration Server and the Managed Servers.

Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topologies outlined in Section 1, "Enterprise Deployment Overview." The topologies and hosts are shown in Table 15–1.

Table 15–1   Hosts in Each Topology

Topology	Hosts
OAM11g	IDMHOST1
	IDMHOST2
OAM11g/OIM11g	IDMHOST1
	IDMHOST2
	OIMHOST1
	OIMHOST2
OIF11g	IDMHOST1
	IDMHOST2
	OIFHOST1
	OIFHOST2

Note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware Home where Node Manager resides). See Section 15.2, "Changing the Location of the Node Manager Log" for further details.

2. Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See Section 15.3, "Enabling Host Name Verification Certificates for Node Manager" for further details.

Note: The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

15.2 Changing the Location of the Node Manager Log

Edit the Node Manager properties file located at *MW_HOME*/wlserver_10.3/common/nodemanager/nodemanager.properties. Add the new location for the log file using the following line:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Oracle best practice is to use a location outside the *MW_HOME* directory and inside the administration directory.

Restart Node Manager, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," for the change to take effect.

15.3 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. It consists of the following steps:

- Section 15.3.1, "Generating Self-Signed Certificates Using the utils.CertGen Utility"

- Section 15.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility"

- Section 15.3.4, "Configuring Node Manager to Use the Custom Keystores"

- Section 15.3.5, "Configuring Managed WebLogic Servers to Use the Custom Keystores"

- Section 15.3.6, "Changing the Host Name Verification Setting for the Managed Servers"

15.3.1 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:

   ```
   HOST> cd WL_HOME/server/bin
   HOST> ./setWLSEnv.sh
   ```

   Verify that the CLASSPATH environment variable is set:

   ```
   HOST> echo $CLASSPATH
   ```

2. Create a user-defined directory for the certificates. For example, create a directory called 'certs' under the *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name* directory. Note that certificates can be shared across WebLogic domains.

   ```
   HOST> cd ORACLE_BASE/admin/domain_name/aserver/domain_name
   HOST> mkdir certs
   ```

   > **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:

   ```
   HOST> cd certs
   ```

4. Run the utils.CertGen tool from the user-defined directory to create the certificates for both *HOST*. mycompany.com and *VIP*. mycompany.com.

   Syntax (all on a single line):

   ```
   java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
   [export | domestic] [Host_Name]
   ```

Examples:

```
IDMHOST1> java utils.CertGen Key_Passphrase IDMHOST1.mycompany.com_cert
IDMHOST1.mycompany.com_key domestic IDMHOST1.mycompany.com

IDMHOST2> java utils.CertGen Key_Passphrase IDMHOST2.mycompany.com_cert
IDMHOST2.mycompany.com_key domestic IDMHOST2.mycompany.com

IDMHOST2> java utils.CertGen Key_Passphrase ADMVHN.mycompany.com_cert
ADMVHN.mycompany.com_key domestic ADMVHN.mycompany.com
```

15.3.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

Follow these steps to create an identity keystore on IDMHOST1:

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, *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name*/certs).

   > **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 IDMHOST1.mycompany.com, IDMHOST2.mycompany.com and ADMVHN.mycompany.com 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:

```
IDMHOST1> java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityIDMHOST1 Key_Passphrase ORACLE_BASE/admin/domain_
name/aserver/domain_name/certs/IDMHOST1.mycompany.com_cert.pem ORACLE_
BASE/admin/domain_name/aserver/domain_name/certs/IDMHOST1.mycompany.com_key.pem

IDMHOST1> java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityIDMHOST2 Key_Passphrase ORACLE_BASE/admin/domain_
name/aserver/domain_name/certs/IDMHOST2.mycompany.com_cert.pem ORACLE_
BASE/admin/domain_name/aserver/domain_name/certs/IDMHOST2.mycompany.com_key.pem

IDMHOST1> java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityADMVHN Key_Passphrase ORACLE_BASE/admin/domain_name/aserver/domain_
name/certs/ADMVHN.mycompany.com_cert.pem ORACLE_BASE/admin/domain_
name/aserver/domain_name/certs/ADMVHN.mycompany.com_key.pem
```

15.3.3 Creating a Trust Keystore Using the Keytool Utility

Follow these steps to create the trust keystore on each host, for example `IDMHOST1` and `IDMHOST2`:

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:

   ```
   IDMHOST1> cp WL_HOME/server/lib/cacerts ORACLE_BASE/admin/domain_
   name/aserver/domain_name/certs/appTrustKeyStoreIDMHOST1.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:

   ```
   HOST> keytool -storepasswd -new New_Password -keystore Trust_Keystore
   -storepass Original_Password
   ```

   For example:

   ```
   IDMHOST1> keytool -storepasswd -new Key_Passphrase -keystore
   appTrustKeyStoreIDMHOST1.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:

   ```
   HOST> keytool -import -v -noprompt -trustcacerts -alias Alias_Name
   -file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
   ```

   For example:

   ```
   IDMHOST1> keytool -import -v -noprompt -trustcacerts -alias clientCACert -file
   WL_HOME/server/lib/CertGenCA.der -keystore appTrustKeyStoreIDMHOST1.jks
   -storepass Key_Passphrase
   ```

15.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the nodemanager.properties file located in the *WL_HOME*/common/nodemanager directory:

```
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=ORACLE_BASE/admin/domain_name/aserver/domain_
name/certs/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentityIDMHOST1
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components." For security reasons, you want to minimize the time the entries in the nodemanager.properties file are left unencrypted. After you edit the file, you should start Node Manager as soon as possible so that the entries get encrypted.

When using a common/shared storage installation for MW_HOME, Node Manager is started from different nodes using the same base configuration (nodemanager.properties). In that case, it is required to add the certificate for all the nodes that share the binaries to the appIdentityKeyStore.jks Identity Store. To do this, create the certificate for the new node and import it to appIdentityKeyStore.jks as in Section 15.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility." Once the certificates are available in the store, each Node Manager must point to a different identity alias to send the correct certificate to the Administration Server. To do this, set different environment variables before starting Node Manager in the different nodes:

```
HOST> cd WL_HOME/server/bin
HOST> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX
```

> **Note:** Make sure to specify the custom identity alias specifically assigned to each host, for example `appIdentity1` for `...HOST1` and `appIdentity2` for `...HOST2`.

15.3.5 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.

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:

     ```
     ORACLE_BASE/admin/domain_name/aserver/domain_
     name/certs/appIdentityKeyStore.jks
     ```

   - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.

   - **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in Section 15.3.3, "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:

   ORACLE_BASE/admin/*domain_name*/aserver/*domain_name*/certs/appTrustKeyStoreIDMHOST1.jks

   ■ **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.

   ■ **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in Section 15.3.3, "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:

   ■ For `wls_ods1`, use `appIdentityIDMHOST1`.

   ■ For `wls_ods2` use `appIdentityIDMHOST2`.

   ■ For `ADMINSERVER` user `appIdentityADMVHN`.

   In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 15.3.2, "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 19.1, "Starting and Stopping Oracle Identity Management Components."

15.3.6 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:

1. Log in to Oracle WebLogic Server Administration Console.

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 Host Name Verifier`.

9. Click **Save**.

10. Click **Activate Changes**.

16

Configuring Server Migration for Oracle Identity Manager

For this high availability topology, you must 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. For this configuration, the `WLS_OIM1`, `WLS_SOA1`, `WLS_OIM2` and `WLS_SOA2` servers listen on specific floating IPs that are failed over by WebLogic Server Migration. Configuring server migration for the Managed Servers consists of the following steps.

The following steps enable server migration for the `WLS_OIM1`, `WLS_SOA1`, `WLS_OIM2`, and `WLS_SOA2` Managed Servers. This enables a Managed Server to fail over to another node in the case of server or process failure.

This chapter contains the following steps:

- Section 16.1, "Setting Up a User and Tablespace for the Server Migration Leasing Table"
- Section 16.2, "Creating a Multi Data Source Using the Oracle WebLogic Administration Console"
- Section 16.3, "Editing Node Manager's Properties File"
- Section 16.4, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"
- Section 16.5, "Configuring Server Migration Targets"
- Section 16.6, "Testing the Server Migration"

16.1 Setting Up a User and Tablespace for the Server Migration Leasing Table

The first step to 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:

```
SQL> 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:

```
SQL> create user leasing identified by welcome1;
SQL> grant create table to leasing;
SQL> grant create session to leasing;
SQL> alter user leasing default tablespace leasing;
SQL> 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 the *WL_HOME*/server/db/oracle/817 or the *WL_HOME*/server/db/oracle/920 directory to your database node.

   b. Connect to the database as the **leasing** user.

   c. Run the leasing.ddl script in SQL*Plus:

   ```
   SQL> @Copy_Location/leasing.ddl;
   ```

16.2 Creating a Multi Data Source Using the Oracle WebLogic Administration Console

The second step is to create a multi data source for the leasing table from the Oracle WebLogic Server Administration Console. You create a data source to each of the Oracle RAC database instances during the process of setting up the multi data source, both for these data sources and the global leasing multi data source. When you create a data source:

- Ensure that this is a non-XA data source.

- The names of the multi data sources are in the format of `MultiDS-rac0`, `MultiDS-rac1`, and so on.

- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11.

- Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource**, **Emulate Two-Phase Commit**, or **One-Phase Commit** options of the **Supports Global Transactions** option), and specify a service name for your database.

- Target these data sources to the `OIM_CLUSTER` and the `SOA_CLUSTER`.

- Ensure the data source's connection pool initial capacity is set to 0 (zero). To do this, select **Services**, **JDBC**, and then **Datasources**. In the Datasources screen, click the **Datasource Name**, then click the **Connection Pool** tab, and enter **0** (zero) in the **Initial Capacity** field.

Creating a Multi Data Source

Perform these steps to create a multi data source:

1. From Domain Structure window in the Oracle WebLogic Server Administration Console, expand the **Services** node. The Summary of JDBC Data Source page appears.

2. Click **Data Sources**. The Summary of JDBC Multi Data Source page is displayed.

3. Click **Lock and Edit**.

4. Click **New Multi Data Source**. The Create a New JDBC Multi Data Source page is displayed.

5. Enter `leasing` as the name.

6. Enter `jdbc/leasing` as the JNDI name.

7. Select **Failover** as algorithm (default).

8. Click **Next.**

9. Select OIM_CLUSTER and SOA_CLUSTER as the targets.

10. Click **Next**.

11. Select **non-XA driver** (the default).

12. Click **Next**.

13. Click **Create New Data Source**.

14. Enter `leasing-rac0` as the name. Enter `jdbc/leasing-rac0` as the JNDI name. Enter `oracle` as the database type. For the driver type, select Oracle Driver (Thin) for Oracle RAC Service-Instance connections, Versions:10 and later.

    > **Note:** When creating the multi data sources for the leasing table, enter names in the format of *MultiDS*-rac0, *MultiDS*-rac1, and so on.

15. Click **Next**.

16. Deselect **Supports Global Transactions**.

17. Click **Next**.

18. Enter the service name, database name, host port, and password for your leasing schema.

19. Click **Next**.

20. Click **Test Configuration** and verify that the connection works.

21. Click **Next**.

22. Target the data source to OIM_CLUSTER and SOA cluster.

23. Select the data source you just created, for example `leasing-rac0`, and add it to the right screen.

24. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the OIM_CLUSTER and SOA_CLUSTER, repeating the steps for the second instance of your Oracle RAC database.

25. Add the second data source to your multi data source.

26. Click **Activate Changes**.

16.3 Editing Node Manager's Properties File

The third step is to edit Node Manager's properties file. This must be done for the Node Managers in both nodes (`OIMHOST1` and `OIMHOST2`) where server migration is being configured:

```
Interface=eth0
NetMask=255.255.255.0
UseMACBroadcast=true
```

- **Interface:** This property specifies the interface name for the floating IP (for example, eth0).

  > **Note:** Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. Node Manager's scripts traverse the different :*X*-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, `eth2`, `eth3`, `eth`*n*, depending on the number of interfaces configured.

- **NetMask:** 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; 255.255.255.0 is used as an example in this document.

- **UseMACBroadcast:** 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
Interface=eth0
NetMask=255.255.255.0
...
```

> **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. Set the following property in the `nodemanager.properties` file:

   - **StartScriptEnabled:** Set this property 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.

> **Note:** When running Node Manager from a shared storage installation, multiple nodes are started using the same `nodemanager.properties` file. However, each node may require different NetMask or Interface properties. In this case, specify individual parameters on a per-node basis using environment variables. For example, to use a different interface (eth3) in HOST*n*, use the Interface environment variable as follows:
>
> ```
> HOSTn> export JAVA_OPTIONS=-DInterface=eth3
> ```
>
> and start Node Manager after the variable has been set in the shell.

16.4 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

This section is not required on Windows. On Linux and UNIX-based systems, the fourth step is to set environment and superuser privileges for the `wlsifconfig.sh` script:

1. Ensure that your PATH environment variable includes these files:

Table 16–1   Files Required for the PATH Environment Variable

File	Located in this directory
wlsifconfig.sh	*ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*/bin/server_migration
wlscontrol.sh	*WL_HOME*/common/bin
nodemanager.domains	*WL_HOME*/common

2. Grant `sudo` configuration for the `wlsifconfig.sh` script.

   - Configure `sudo` to work without a password prompt.

   - 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:

   - Grant `sudo` privilege to the WebLogic user `oracle` with no password restriction, and grant execute privilege on the `/sbin/ifconfig and /sbin/arping` binaries.

   - Ensure 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`:

     ```
     oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
     ```

   > **Note:** Ask the system administrator for the appropriate `sudo` and system rights to perform this step.

16.5 Configuring Server Migration Targets

The sixth step is to configure server migration targets. You first assign all the available nodes for the cluster's members and then specify candidate machines (in order of

preference) for each server that is configured with server migration. Follow these steps to configure cluster migration in a migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console (http://*Host*:*Admin_Port*/console). Typically, *Admin_Port* is 7001 by default.

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 machine to which to allow migration and click the right arrow. In this case, select **OIMHOST1** and **OIMHOST2**.

7. Select the data source to be used for automatic migration. In this case, select the leasing data source.

8. Click **Save**.

9. Click **Activate Changes**.

10. Repeat steps 2 through 9 for the SOA cluster.

11. Set the candidate machines for server migration. You must perform this task for all of the Managed Servers as follows:

    a. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.

       Tip: Click **Customize this table** in the Summary of Servers page and move Current Machine from the Available window to the Chosen window to view the machine on which the server is running. This is different from the configuration if the server gets migrated automatically.

    b. Select the server for which you want to configure migration.

    c. Click the **Migration** tab.

    d. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow. For **WLS_OIM1**, select **OIMHOST2**. For **WLS_OIM2**, select **OIMHOST1**.

    e. Select **Automatic Server Migration Enabled**. This enables Node Manager to start a failed server on the target node automatically.

    f. Click **Save**.

    g. Click **Activate Changes**.

    h. Repeat the previous steps for the WLS_SOA1 and WLS_SOA2 Managed Servers.

    i. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured.

16.6 Testing the Server Migration

The final step is to test the server migration. Perform these steps to verify that server migration is working properly:

From OIMHOST1:

1. Stop the WLS_OIM1 Managed Server. To do this, run this command:

   ```
   OIMHOST1> 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:

   ```
   OIMHOST1> ps -ef | grep WLS_OIM1
   ```

2. Watch the Node Manager console. 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.

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 soa-infra console in the same IP.

Follow the previous steps to test server migration for the WLS_OIM2, WLS_SOA1, and WLS_SOA2 Managed Servers.

Table 16–2 shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 16–2   WLS_OIM1, WLS_OIM2, WLS_SOA1, WLS_SOA2 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 Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.

2. Click **Domain** on the left console.

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 Managed Server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the Managed Server on the machine to which it was originally assigned.

17

Integrating Components

This chapter contains the following topics:

17.1 Fusion Applications Provisioning

Once the complete environment is set up, perform the following step to prepare the environment for Fusion Applications provisioning.

This section contains the following topics:

17.1.1 Input to the Fusion Applications Provisioning Tool

In the previous chapters, when you run `idmConfigTool`, the command writes the parameters that are required for Fusion Applications provisioning in the file `idmDomainConfig.param`. You use this file as a input to the Fusion Applications provisioning tool.

In addition, since the Fusion Applications domain must interact with the Identity Management domain in SSL mode, you must provide a keystore containing the Trust point used by the Identity Management domain to the Fusion Applications. You do this by following the steps in the next section.

> **Note:**
>
> If you are using Windows, you must install a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See `http://www.cygwin.com`.
>
> When using Cygwin, ensure that you use the "/" character in path names when exporting a variable. For example:
>
> ```
> export ORACLE_HOME=c:/oracle/idm
> ```

17.1.2 Creating Client Certificate

To enable Fusion Applications to communicate with the Identity Management domain using SSL Server Authentication Mode, you must generate a client certificate and provide it to the Fusion Applications Provisioning process. To generate this certificate perform the following steps:

1. Set the `ORACLE_HOME` and `JAVA_HOME` variables. For example, on `OIDHOST1`, issue these commands:

   ```
   export ORACLE_HOME=IDM_ORACLE_HOME
   export PATH=$JAVA_HOME/bin:$PATH
   ```

2. To generate the certificate, use the tool `./SSLClientConfig.sh`, which is located in:

   `ORACLE_COMMON_HOME/bin`

   For example

   ```
   ./SSLClientConfig.sh -component cacert
   ```

   As the command runs, enter the following values when prompted:

   - LDAP Host Name: `policystore.mycompany.com`
   - LDAP Port: `389`
   - LDAP User: `cn=orcladmin`
   - Password: `Password_for_cn=orcladmin`
   - SSL Domain: `IDMDomain`
   - Keystore Password: Enter a password to protect the keystore
   - Confirm Password: Reenter the password.

   The following is typical output from the command:

   ```
   ./SSLClientConfig.sh -component cacert
   SSL Automation Script: Release 11.1.1.4.0 - Production
   Copyright (c) 2010 Oracle. All rights reserved.
   Downloading the CA certificate from a central LDAP location
   Creating a common trust store in JKS and Oracle Wallet formats ...
   Configuring SSL clients with the common trust store...
   Make sure that your LDAP server is currently up and running.
   Downloading the CA certificate from the LDAP server...
   >>>Enter the LDAP hostname [oidhost1.mycompany.com]: policystore.mycompany.com
   >>>Enter the LDAP port: [3060]? 389
   >>>Enter your LDAP user [cn=orcladmin]:
   >>>Enter password for cn=orcladmin:
   >>>Enter the sslDomain for the CA [idm]: IDMDomain
   >>>Searching the LDAP for the CA usercertificate ...
   Importing the CA certifcate into trust stores...
   >>>The common trust store in JKS format is located at
    /u01/app/oracle/product/fmw/IDM/rootCA/keystores/tmp/trust.jks
   >>>The common trust store in Oracle wallet format is located at
   /u01/app/oracle/product/fmw/IDM/rootCA/keystores/tmp/ewallet.p12
   Generate trust store for the CA cert at cn=IDMDomain,cn=sslDomains
   >>>Enter a password to protect your truststore:
   >>>Enter confirmed password for your truststore:

   Create directory /u01/app/oracle/product/fmw/IDM/rootCA/keystores/common
   Importing the CA certifcate into trust stores...
   ```

```
>>>The common trust store in JKS format is located at
/u01/app/oracle/product/fmw/IDM/rootCA/keystores/common/trust.jks
>>>The common trust store in Oracle wallet format is located at
/u01/app/oracle/product/fmw/IDM/rootCA/keystores/common/ewallet.p12
```

This creates a file called `trust.jks` which must be provided to the Fusion Applications Provisioning process. After creating this certificate, you must delete the private key within this key. Use the following command:

```
keytool -delete -keystore trust.jks -alias testkey -storepass store_password
```

17.2 Integrating Oracle Identity Manager and Oracle Access Manager 11g

This section describes how to integrate Oracle Identity Manager and Oracle Access Manager 11*g*.

This section contains the following topics:

- Section 17.2.1, "Prerequisites"
- Section 17.2.2, "Copying OAM Keystore Files to OIMHOST1 and OIMHOST2"
- Section 17.2.3, "Configuring Oracle Access Manager for Oracle Identity Manager Integration"
- Section 17.2.4, "Updating Existing LDAP Users with Required Object Classes"
- Section 17.2.5, "Integrating Oracle Access Manager 11g with Oracle Identity Manager 11g"
- Section 17.2.6, "Validating Integration"

17.2.1 Prerequisites

1. Ensure that OIM11g has been installed and configured as described in Chapter 13, "Extending the Domain with Oracle Identity Manager."

2. Ensure that the Oracle Access Manager 11g has been installed and configured as described in Chapter 12, "Extending the Domain with Oracle Access Manager 11g."

3. Ensure that OHS has been installed and configured as described in Chapter 4.4, "Installing Oracle HTTP Server."

4. Ensure that the JTA Transaction Timeout for the domain is 600 seconds or greater. If required update the timeout value by following these steps:

   a. Open a browser and go to the WebLogic Administration Console at:
      `http://admin.mycompany.com/console`

   b. Log in to the WebLogic Administrative Console as an administrative user.

   c. Navigate to **Services** -> **JTA**.

   d. If the value for **Timeout Seconds** less than `600`, click **Lock** and **Edit**, then update the value to `600`.

   e. Click **Save**.

   f. Click **Activate Changes**.

   g. Stop the Administration Server and the Managed Servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

    h. Start the Administration Server using Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

    i. Start the Managed Servers in your domain using the WebLogic Administration Console as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

17.2.2 Copying OAM Keystore Files to OIMHOST1 and OIMHOST2

If you are using Oracle Access Manager with the Simple Security Transport model, you must copy the OAM keystore files that were generated in Section 12.9, "Creating Oracle Access Manager Key Store" to `OIMHOST1` and `OIMHOST2`. Copy the keystore files `ssoKeystore.jks` and `oamclient-truststore.jks` to the directory `DOMAIN_HOME`/config/fmwconfig on `OIMHOST1` and `OIMHOST2`.

17.2.3 Configuring Oracle Access Manager for Oracle Identity Manager Integration

Before integrating Oracle Identity Manager with Oracle Access Manager 11g, you must extend Oracle Access Manager 11g to support Oracle Identity Manager.

To do this, perform the following tasks on `IDMHOST1`

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.

2. Create a properties file called `config_oam2.props` with the following contents:

```
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
WLSPASSWD: weblogic password
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: oamhost1.mycompany.com:5575,oamhost2.mycompany.com:5575
WEBGATE_TYPE: ohsWebgate10g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.mycompany.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM_TRANSFER_MODE: simple
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_OIM_WEBGATE_PASSWD: webgate password
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
COOKIE_DOMAIN: .us.oracle.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
```

```
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_IMPERSONATION_FLAG:true
OAM11G_SERVER_LBR_HOST:sso.mycompany.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_OIM_OHS_URL:https://sso.mycompany.com:443/
```

Where:

- `WLSHOST` and `WLSPORT` are, respectively, the host and port of your administration server, created in Chapter 6, "Creating the WebLogic Server Domain for Identity Management." This is the virtual name.

- `WLSADMIN` and `WLSPASSWD` are, respectively, the WebLogic administrative user and password you use to log in to the WebLogic console.

- `IDSTORE_HOST` and `IDSTORE _PORT` are, respectively, the host and port of your Identity Store directory.

- `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.

- `IDSTORE_USERSEARCHBASE` is the container under which Oracle Access Manager searches for the users.

- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are stored.

- `IDSTORE_SEARCHBASE` is the location in the directory where Users and Groups are stored.

- `IDSTORE_OAMSOFTWAREUSER` is the name of the user you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager" to be used to interact with LDAP.

- `IDSTORE_OAMADMINUSER` is the name of the user you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager" to access your OAM Console.

- `PRIMARY_OAM_SERVERS` is a comma separated list of your Oracle Access Manager Servers and the proxy ports they use.

> **Note:** To determine the proxy ports your OAM Servers use:
>
> 1. Log in to the OAM console at `http://admin.mycompany.com:7001/oamconsole`
> 2. Click the **System Configuration** tab.
> 3. Expand **Server Instances** under the Common Configuration section
> 4. Click an Oracle Access Manager server, such as **WLS_OAM1**, and click **Open**.
> 5. Proxy port is the one shown as **Port**.

- `ACCESS_GATE_ID` is the name you want to assign to the WebGate.

- `OAM11G_OIM_WEBGATE_PASSWD` is the password you want to assign to the WebGate.

- `OAM11G_IDM_DOMAIN_OHS_HOST` is the name of the load balancer which is in front of the OHS's.

- `OAM11G_IDM_DOMAIN_OHS_PORT` is the port that the load balancer listens on.

- `OAM11G_IDM_DOMAIN_OHS_PROTOCOL` is the protocol to use when directing requests at the load balancer.

- `OAM11G_OAM_SERVER_TRANSFER_MODE` is the security model that the Access Servers function in, as defined in Section 12.6.1, "Changing Oracle Access Manager Security Model."

- `OAM11G_IMPERSONATION_FLAG` is set to `True` if you are using Oracle Fusion Applications.

- `OAM11G_IDM_DOMAIN_LOGOUT_URLS` is set to the various logout URLs.

- `OAM11G_SSO_ONLY_FLAG` configures Oracle Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization. This is set to `true` for Fusion Applications.

  If `OAM11G_SSO_ONLY_FLAG` is `true`, the Oracle Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Oracle Access Manager server.

  If the value is `false`, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Oracle Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Oracle Access Manager server.

- `OAM11G_SERVER_LBR_HOST` is the name of the load balancer fronting your site. This and the following two parameters are used to construct your login URL.

- `OAM11G_SERVER_LBR_PORT` is the port that the load balancer is listening on.

- `OAM11G_SERVER_LBR_PROTOCOL` is the URL prefix to use.

- `COOKIE_DOMAIN` is the domain in which the WebGate functions.

- `WEBGATE_TYPE` is the type of WebGate agent you want to create. Valid values are `ohsWebgate10g` and `ohsWebgate11g`.

- `OAM11G_IDSTORE_NAME` is the name of the Identity Store. If you already have an Identity Store in place which is different from the default created by this tool, set this parameter to the name of that Identity Store.

3. Configure Oracle Access Manager using the command `idmConfigTool`, which is located at *IAM_ORACLE_HOME*/idmtools/bin.

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

IAM_ORACLE_HOME/idmtools/bin

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOAM input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -configOAM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOAM input_file=config_oam2.props
```

When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to the accounts:

- `IDSTORE_PWD_OAMSOFTWAREUSER`

- `IDSTORE_PWD_OAMADMINUSER`

Sample command output:

```
Enter ID Store Bind DN password :
Enter User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Confirm User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Enter User Password for IDSTORE_PWD_OAMADMINUSER:
Confirm User Password for IDSTORE_PWD_OAMADMINUSER:
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them

5. Restart WebLogic Administration Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

17.2.4 Updating Existing LDAP Users with Required Object Classes

You must update existing LDAP users with the object classes `OblixPersonPwdPolicy`, `OIMPersonPwdPolicy`, and `OblixOrgPerson`.

> **Note:** This is not required in the case of a fresh setup where you do not have any existing users.

On `IDMHOST1`, create a properties file for the integration called `user.props`, with the following contents:

```
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_ADMIN_USER: cn=orcladmin
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
PASSWORD_EXPIRY_PERIOD : 7300
```

Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

Set `IDM_HOME` to `IDM_ORACLE_HOME`.

Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.

Upgrade existing LDAP, using the command `idmConfigTool`, which is located at: *IAM_ORACLE_HOME*/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command is:

```
idmConfigTool.sh - upgradeLDAPUsersForSSO input_file=configfile
```

on Linux and UNIX-based operating systems and

```
idmConfigTool.bat -upgradeLDAPUsersForSSO input_file=configfile
```

on Windows.

For example:

```
idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=user.props
```

When prompted, enter the following information:

- The password of the user you are using to connect to your Identity Store.
- The directory type: `OVD` if you are using Oracle Virtual Directory, otherwise `OID`

Sample output:

```
Enter LDAP admin user password :


********* Upgrading LDAP Users With OAM ObjectClasses *********

Enter Directory Type[OID]: OVD

Completed loading user inputs for - LDAP connection info

Completed loading user inputs for - LDAP Upgrade

Upgrading ldap users at - cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it
```

```
objectclass OblixOrgPerson not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com


Parsing - cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com
```

```
Parsing - cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=PUBLIC, cn=Users, dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PUBLIC, cn=Users, dc=us,dc=oracle,dc=com

Parsing - cn=orcladmin, cn=Users, dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in cn=orcladmin, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=orcladmin, cn=Users, dc=us,dc=oracle,dc=com

Parsing - cn=xelsysadm,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=xelsysadmin,cn=Users,dc=us,dc=oracle,dc=com

Finished parsing LDAP

LDAP Users Upgraded.

********* ********* *********
```

> **See Also:** *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

17.2.5 Integrating Oracle Access Manager 11*g* with Oracle Identity Manager 11*g*

This section describes how to integrate Oracle Access Manager 11g with Oracle Identity Manager

17.2.5.1 Remove Security Providers

If you have previously performed the tasks in Section 18, "Configuring Single Sign-on for Administration Consoles," you must delete the security providers you created in that section.

To do this:

1. Log in to the WebLogic Administration Console at:

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

2. Click **Security Realms** from the Domain structure menu.

3. Click **Lock** and **Edit** in the Change Center.

4. Click **myrealm**.

5. Select the **Providers** tab.

   Select the following providers:

   - **OVDAuthenticator**

   - **OIDAuthenticator**

   - **OAMIDAssertor**

6. Click **Delete**.

7. Click **Yes** to confirm deletion.

8. Restart the administration server and all managed servers, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

17.2.5.2 Integrating Oracle Access Manager with Oracle Identity Manager by Using idmConfigTool

To integrate Oracle Access Manager 11*g* with Oracle Identity Manager perform the following steps on `IDMHOST1`:

1. Set the Environment Variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME`, and `ORACLE_HOME`, for example:

   ```
   export IDM_HOME=IDM_ORACLE_HOME
   export ORACLE_HOME=IAM_ORACLE_HOME
   ```

2. Create a properties file for the integration called `oimitg.props`, with the following contents:

   ```
   LOGINURI: /${app.context}/adfAuthentication
   LOGOUTURI: /oamsso/logout.html
   AUTOLOGINURI: None
   ACCESS_SERVER_HOST: OAMHOST1.mycompany.com
   ACCESS_SERVER_PORT: 5575
   ACCESS_GATE_ID: Webgate_IDM
   COOKIE_DOMAIN: .mycompany.com
   COOKIE_EXPIRY_INTERVAL: 120
   OAM_TRANSFER_MODE: simple
   WEBGATE_TYPE: ohsWebgate10g
   SSO_ENABLED_FLAG: true
   IDSTORE_PORT: 389
   IDSTORE_HOST: idstore.mycompany.com
   IDSTORE_DIRECTORYTYPE: OID or OVD
   IDSTORE_ADMIN_USER: cn=oamLDAP,cn=Users,dc=mycompany,dc=com
   IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
   MDS_DB_URL: jdbc:oracle:thin:@(DESCRIPTION=(LOAD_
   BALANCE=on)(FAILOVER=on)(ADDRESS_
   LIST=(ADDRESS=(protocol=tcp)(host=OIDDBHOST1-vip.mycomapny.com)(port=1521))(ADD
   RESS=(protocol=tcp)(host=OIDDBHOST2-vip.mycompany.com)(port=1521)))(CONNECT_
   DATA=(SERVER=DEDICATED)(SERVICE_NAME=oidedg.mycompany.com)))
   MDS_DB_SCHEMA_USERNAME: edg_mds
   WLSHOST: adminvhn.mycompany.com
   WLSPORT: 7001
   ```

```
WLSADMIN: weblogic
DOMAIN_NAME: IDMDomain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
```

> **Notes:**
>
> - Set `IDSTORE_HOST` to your Oracle Internet Directory host or load balancer name if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory host or load balancer name.
>
> - Set `IDSTORE_DIRECTORYTYPE` to `OVD` if you are using Oracle Virtual Directory server to connect to either a non-OID directory or Oracle Internet Directory. Set it to `OID` if your Identity Store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory.
>
> - If your access manager servers are configured to accept requests using the simple mode, set `OAM_TRANSFER_MODE` to `simple`. Otherwise set `OAM_TRANSFER_MODE` to `open`
>
> - Set `IDSTORE_PORT` to your Oracle Internet Directory port if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory port.
>
> - If you are using a single instance database, then set `MDS_URL` to: `jdbc:oracle:thin:@DBHOST:1521:SID`

3. Change location to: *IAM_ORACLE_HOME*/server

```
cd IAM_ORACLE_HOME/server
```

4. Integrate Oracle Access Manager with Oracle Identity Manager using the command `idmConfigTool`, which is located at:

IAM_ORACLE_HOME/idmtools/bin

> **Note:** When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command is

```
idmConfigTool.sh -configOIM input_file=configfile
```

on Linux and UNIX-based systems, and

```
idmConfigTool.bat -configOIM input_file=configfile
```

on Windows.

For example:

IAM_ORACLE_HOME/idmtools/bin/idmConfigTool.sh -configOIM input_

```
file=oimitg.props
```

When the script runs you are prompted for:

- Access Gate Password

- SSO Keystore Password

- Global Passphrase

- Idstore Admin Password

- MDS Database schema password

- Admin Server User Password

Sample output:

```
Enter sso access gate password :
Enter mds db schema password :
Enter idstore admin password :
Enter admin server user password :

********* Seeding OAM Passwds in OIM *********

Enter ssoKeystore.jks Password:
Enter SSO Global Passphrase:

Completed loading user inputs for - CSF Config

Updating CSF with Access Gate Password...

WLS ManagedService is not up running. Fall back to use system properties for
configuration.
Updating CSF ssoKeystore.jks Password...

Updating CSF for SSO Global Passphrase Password...


********* ********* *********


********* Activating OAM Notifications *********


Completed loading user inputs for - MDS DB Config

Initialized MDS resources

Apr 11, 2011 4:57:45 AM oracle.mds
NOTIFICATION: transfer operation started.
Apr 11, 2011 4:57:46 AM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
Upload to DB completed


Releasing all resources

Notifications activated.


********* ********* *********
```

```
********* Seeding OAM Config in OIM *********

Completed loading user inputs for - OAM Access Config

Validated input values

Initialized MDS resources

Apr 11, 2011 4:57:46 AM oracle.mds
NOTIFICATION: transfer operation started.
Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
Download from DB completed

Releasing all resources

Updated /u01/app/oracle/product/fmw/IAM/server/oamMetadata/db/oim-config.xml

Initialized MDS resources

Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: transfer operation started.
Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
Upload to DB completed


Releasing all resources

OAM configuration seeded. Please restart oim server.


********* ********* *********


********* Configuring Authenticators in OIM WLS *********
Completed loading user inputs for - Dogwood Admin WLS


Completed loading user inputs for - LDAP connection info

Connecting to t3://adminvhn.mycompany.com:7001

Connection to domain runtime mbean server established

Starting edit session

Edit session started

Connected to security realm.

Validating provider configuration

Validated desired authentication providers

Validated authentication provider state successfuly.
```

```
Created OAMIDAsserter successfuly

Created OIDAuthenticator successfuly

Created OIMSignatureAuthenticator successfuly

Setting attributes for OID Authenticator

All attributes set. Configured in OID Authenticator now

lDAP details configured in OID authenticator

Control flags for authenticators set sucessfully

Reordering of authenticators done sucessfully

Saving the transaction

Transaction saved

Activating the changes

Changes Activated. Edit session ended.

Connection closed sucessfully


********* ********* *********
```

> **Note:** If you have already enabled single sign-on for your WebLogic
> Administration Consoles as described in Section 18.1, "Configuring
> Single Sign-On for Administration Consoles with Oracle Access
> Manager 11g" when this script is run, you might see the following
> errors when this script is run:
>
> ```
> ERROR: Desired authenticators already present.
> [Ljava.lang.String;@7fdb492]
> ERROR: Error occurred while configuration. Authentication providers
> to be configured already present.
> ERROR: Rolling back the operation..
> ```
>
> These errors can be ignored.

5. Check the log file for errors and correct them if necessary.

6. Restart `WLS_OIM1`, `WLS_OIM2`, and the WebLogic Administration Server, as
   described in Section 19.1, "Starting and Stopping Oracle Identity Management
   Components."

17.2.6 Validating Integration

To validate integration, you must assign Identity Management administrators to
WebLogic security groups and install WebGate as described in Chapter 18,
"Configuring Single Sign-on for Administration Consoles."

To validate that the wiring of Oracle Access Manager 11g with Oracle Identity Manager 11g was successful, attempt to log in to the Oracle Identity Manager Self Service Console, as follows:

1. Using a browser, navigate to `https://sso.mycompany.com/oim`. This redirects you to the OAM11g single sign-on page.

2. Log in using the `xelsysadm` user account created in Section 11.4.3, "Creating Users and Groups for Oracle Identity Manager."

3. If you see the OIM Self Service Console Page, the integration was successful.

17.3 Integrating Oracle Identity Federation with Oracle Access Manager 11*g*

Oracle Identity Federation supports two integration modes with Oracle Access Manager: authentication mode and SP mode.

Authentication Mode (IdP)

In the authentication mode, Oracle Identity Federation delegates authentication of the user to Oracle Access Manager.

The user is redirected to an Oracle Identity Federation resource protected by WebGate, that triggers the Oracle Access Manager authentication flow. Once the user is identified, it will access the resource, and WebGate will provide to Oracle Identity Federation an HTTP header containing the user's identity.

SP Mode

In the SP mode, Oracle Access Manager delegates user authentication to Oracle Identity Federation, which uses the Federation Oracle Single Sign-On protocol with a remote Identity Provider. Once the Federation Oracle Single Sign-On flow is performed, Oracle Identity Federation will create a local session and then propagates the authentication state to Oracle Access Manager, which maintains the session information.

This section provides the steps to integrate OIF with OAM11g in authentication mode and SP mode.

This section contains the following topics:

- Section 17.3.1, "Prerequisites"

- Section 17.3.2, "Integrating Oracle Identity Federation with Oracle Access Manager in Authentication Mode"

- Section 17.3.3, "Integrating Oracle Identity Federation with Oracle Access Manager in SP Mode"

- Section 17.3.4, "Validating Oracle Identity Federation Integration with Oracle Access Manager"

17.3.1 Prerequisites

Before starting this integration, ensure that the following tasks have been performed:

- Install and configure Oracle Identity Federation as described in Chapter 14, "Extending the Domain with Oracle Identity Federation."

- Install and configure Oracle Access Manager as described in Chapter 12, "Extending the Domain with Oracle Access Manager 11g."

- Install and configure Oracle HTTP Server as described in Section 4.4, "Installing Oracle HTTP Server."

- Install and configure WebGate as described in Section 18.5, "Installing and Configuring WebGate."

17.3.2 Integrating Oracle Identity Federation with Oracle Access Manager in Authentication Mode

This section covers the following topics:

- Section 17.3.2.1, "Creating an Authorization Policy in Oracle Access Manager"

- Section 17.3.2.2, "Creating a Resource in Oracle Access Manager"

- Section 17.3.2.3, "Configuring the Oracle Access Manager Authentication Engine"

- Section 17.3.2.4, "Configuring the OSSO SP Engine"

17.3.2.1 Creating an Authorization Policy in Oracle Access Manager

Create an Authorization Policy in Oracle Access Manager to enable local authorization for Oracle Identity Federation. To create an authorization policy, log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the OAM administration user. Then perform the following steps:

1. Click the **Policy Configuration** tab.

2. Expand **IAM Suite** under the Application Domains section.

3. Click **Authorization Policies**, and then select **Create** from the menu.

4. On the Authorization Policy page, provide the following details:

   - **Name**: The name of the authorization policy, for example: `OIF Local Authorization`

   - **Description**: The description for the policy

5. Click the **Responses** tab, then click **+** to add the HTTP Header Attributes. Enter the following information:

   - **Name**: Enter `OAM_REMOTE_USER` as the name. Make a note of this name, as it is used when configuring the Authentication Engines in the next section.

   - **Type**: `Header`

   - **Value**: `$user.attr.uid`

6. Click **Apply**.

17.3.2.2 Creating a Resource in Oracle Access Manager

Create a resource for the OIF URL to be protected by Oracle Access Manager for authentication. To create a resource, log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the OAM administration user. Then perform the following steps:

1. Click the **Policy Configuration** tab.

2. Expand **IAM Suite** under the Application Domains section.

3. Click **Resources**, and then select **Open** from the menu.

4. On the IAM Suite Resources page, Click **New Resources** to bring up the Resources page.

5. On the Resources Page, provide the following details:

   ■ **Type**: Select HTTP

   ■ **Host Identifier**: IAMSuiteAgent

   ■ **Resource URL**: /fed/user/authnoam

   ■ **Protection Level**: Protected

   ■ **Authorization Policy**: Select the Authorization Policy created in Section Section 17.3.2.1, "Creating an Authorization Policy in Oracle Access Manager," for example: OIF Local Authorization.

   ■ **Authentication Policy**: Protected Higher Level Policy.

   ■ **Query String**: Leave blank

6. Click **Apply**.

17.3.2.3 Configuring the Oracle Access Manager Authentication Engine

Configure Oracle Identity Federation's Oracle Access Manager Authentication engine to protect Oracle Identity Federation with an Oracle Access Manager 11g WebGate. To configure the authentication engine, log in to Oracle Enterprise Manager Fusion Middleware Control at http://admin.mycompany.com/em as the WebLogic administration user. Then perform the following steps:

1. Locate and select the **Oracle Identity Federation** instance under Identity and Access.

2. Navigate to **Administration**, then **Authentication Engines**.

3. Select **Enable Authentication Engine** to enable the Oracle Access Manager Authentication engine.

4. Enter OAM_REMOTE_USER as the **User Unique ID Header**.

5. Select Oracle Access Manager as the Default Authentication Engine from the list.

6. Do **not** select Logout Enabled, since the logout will be performed with the Oracle Single Sign-On SP Engine.

7. Click **Apply** to apply the changes.

17.3.2.4 Configuring the OSSO SP Engine

You must configure the OSSO SP Engine, even though none of the SP functionality is used. This is required because the Logout flow between Oracle Identity Federation and Oracle Access Manager uses the OSSO SP Engine.

Configure the OSSO SP Engine as described in Section 17.3.3.1, "Configuring the OSSO SP Engine."

17.3.3 Integrating Oracle Identity Federation with Oracle Access Manager in SP Mode

This section covers the following topics:

■ Section 17.3.3.1, "Configuring the OSSO SP Engine"

■ Section 17.3.3.2, "Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager"

- Section 17.3.3.3, "Creating an Oracle Identity Federation Authentication Policy in Oracle Access Manager"

- Section 17.3.3.4, "Creating a Resource in Oracle Access Manager"

- Section 17.3.3.5, "Configuring Oracle Access Manager to Delegate Authentication to Oracle Identity Federation"

17.3.3.1 Configuring the OSSO SP Engine

In SP mode, Oracle Identity Federation uses federation protocols to authenticate a user, and then requests the authentication module to create an authenticated session at Oracle Access Manager. Oracle Identity Federation's Single Sign-On SP engine is used for this purpose. The SSO SP engine also provides logout integration. The Oracle Single Sign-On SP engine must be updated with the OAM Server details to enable OIF to send assertion tokens and direct session management to OAM.

To update the Oracle Single Sign-On SP engine, log in to Oracle Enterprise Manager Fusion Middleware Control at `http://admin.mycompany.com/em` as the WebLogic administration user. Then perform the following steps:

1. Locate and select the **Oracle Identity Federation** instance under Identity and Access.

2. Navigate to **Administration**, then **Service Provider Integration Modules**.

3. Select the **Oracle Single Sign-On** tab.

4. Select **Enable SP Module** to enable the Oracle Single Sign-On SP engine.

5. Provide the following details:

   - **Username Attribute**: `cn`

   - **Login URL**: `https://sso.mycompany.com/oam/server/dap/cred_submit`

   - **Logout URL**: `https://sso.mycompany.com/oam/server/logout`

6. Select **Logout Enabled**.

7. Click **Apply** to update the Oracle Single Sign-On SP Engine.

8. Click **Regenerate** to generate a keystore file. This keystore contains the keys used to encrypt and decrypt the tokens that are exchanged between the Oracle Access Manager and Oracle Identity Federation servers.

9. Save the keystore file using the **Save As** dialog.

10. Copy the keystore file to user defined location on `IDMHOST1`. This keystore will be used to register Oracle Identity Federation as Delegated Authentication Protocol (DAP) partner in the next section.

17.3.3.2 Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager

Oracle Access Manager ships with an Oracle Identity Federation Authentication Scheme. This scheme needs to be updated before it can be used. To update the scheme, log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the OAM administration user. Then perform the following steps:

1. Click the **Policy Configuration** tab.

2. Expand **Authentication Schemes** under the Shared Components tree.

3. Select **OIFScheme** from under the Authentication Schemes and then select **Open** from the menu.

4. On the Authentication Schemes page, provide the following information

   ■ **Challenge URL**: `https://sso.mycompany.com:443/fed/user/sposso`

   ■ **Context Type**: Select **external** from the list.

   Accept the defaults for all other values

5. Click **Apply** to update the `OIFScheme`.

17.3.3.3 Creating an Oracle Identity Federation Authentication Policy in Oracle Access Manager

Create an authentication policy in Oracle Access Manager to enable OIF to authenticate the user. To create an authentication policy, log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the OAM administration user. Then perform the following steps:

1. Click the **Policy Configuration** tab.

2. Expand **IAM Suite** under the Application Domains section.

3. Click **Authentication Policies**, and then select **Create** from the menu.

4. On the Authentication Policy page, provide the following details:

   ■ **Name**: The name of the authentication policy, for example: `OIF Policy`.

   ■ **Description**: The description for the policy

   ■ **Authentication Scheme**: Select **OIF Scheme** from the menu

5. Click **Apply**.

17.3.3.4 Creating a Resource in Oracle Access Manager

Create a resource for the Oracle Identity Federation URL to be protected by Oracle Access Manager. In SP mode, Oracle Identity Federation authenticates the user and then propagates the authentication state to Oracle Access Manager. The resource created here is for the purposes of testing.

To create a resource, log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the OAM administration user. Then perform the following steps:

1. Click the **Policy Configuration** tab.

2. Expand **IAM Suite** under the Application Domains section.

3. Click **Resources**, and then select **Open** from the menu.

4. On the IAM Suite Resources page, click **New Resources** to bring up the Resources page.

5. On the Resources page, provide the following details:

   ■ **Type**: Select **HTTP**

   ■ **Host Identifier**: `IAMSuiteAgent`

   ■ **Resource URL**: `/sso.html`

   ■ **Protection Level**: **Protected**

   ■ **Authorization Policy**: **Protected Resource Policy**

- **Authentication Policy**: Select the Authentication Policy created in Section 17.3.3.3, "Creating an Oracle Identity Federation Authentication Policy in Oracle Access Manager," for example: **OIF Policy**.

6. Click **Apply**.

17.3.3.5 Configuring Oracle Access Manager to Delegate Authentication to Oracle Identity Federation

The Oracle Identity Federation resources protected by Oracle WebGate are directed to Oracle Access Manager for authentication. In SP Mode, Oracle Identity Federation authenticates the user and propagates the authentication state to Oracle Access Manager. To enable Oracle Identity Federation to authenticate the user, Oracle Access Manager must be configured to redirect the user to Oracle Identity Federation for authentication. This is done by registering Oracle Identity Federation as Delegated Authentication Protocol (DAP) partner with Oracle Access Manager.

Proceed as follows on IDMHOST1 to register Oracle Identity Federation as DAP Partner with Oracle Access Manager:

1. Ensure that the keystore generated in the previous section is available on IDMHOST1.

2. Start the wlst shell from the *IAM_ORACLE_HOME*/common/bin directory. For example, on Linux and UNIX-based systems, you would type:

   ```
   ./wlst.sh
   ```

   On Windows you would type:

   ```
   ./wlst.cmd
   ```

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://ADMINVHN.mycompany.com:7001")
   ```

4. Use the registerOIFDAPPartner command to register Oracle Identity Federation as a DAP partner with Oracle Access Manager.

   The syntax is:

   ```
   registerOIFDAPPartner(keystoreLocation="path_to_keystore", logoutURL="OIF_logout_URL", rolloverTime="")
   ```

   where:

   - *path_to_keystore* is the location of the Keystore file on IDMHOST1, for example: /home/oracle/keystore

   - *OIF_logout_URL* is the OIF Server's logout URL. Use

     https://*oifhost*:*oifport*/fed/user/sploosso?doneURL=https://*oamhost*:*oam port*/oam/logout.jsp as the logout URL

     Use sso.mycompany.com as the value for *oifhost* and *oamhost*.

     Use 443 as the value for *oifport* and *oamport*.

- ■ *rollover_time* is the rollover interval for the keys used to encrypt ordecrypt SASSO tokens.

For example:

```
wls:/IDMDomain/serverConfig>
registerOIFDAPPartner(keystoreLocation="/home/oracle/keystore",
logoutURL="https://sso.mycompany.com/fed/user/spsloosso?doneURL=https://sso.myc
ompany.com/oam/logout.jsp")

Registration Successful
```

5. Restart the Administration Server and the Oracle Access Manager and Oracle Identity Federation Managed Servers by following the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

17.3.4 Validating Oracle Identity Federation Integration with Oracle Access Manager

Before the configuration can be validated, obtain the provider metadata and register the providers. For the purposes of validating, Oracle Identity Federation will act as both an Identity Provider and a Service Provider.

17.3.4.1 Generating Provider Metadata

Proceed as follows to generate the IdP and SP metadata.

Log in to Oracle Enterprise Manager Fusion Middleware Control at `http://admin.mycompany.com/em` as the WebLogic administration user. Then perform the following steps:

1. Locate and select the **Oracle Identity Federation** instance under Identity and Access.

2. Navigate to **Administration**, then **Security and Trust**.

3. Select the **Provider Metadata** tab.

4. Under the Generate Metadata section:

   a. Select **Service Provider** from the **Provider Type** list.

   b. Click to Generate metadata for the service provider.

   c. Save the generated file using the **Save File** option.

   d. Select **Identity Provider** from the **Provider Type** list.

   e. Click to Generate metadata for the identity provider.

   f. Save the generated file using the **Save File** option.

17.3.4.2 Registering the Providers

Proceed as follows to register the IdP and SP providers using the metadata generated in the previous section.

Log in to Oracle Enterprise Manager Fusion Middleware Control at `http://admin.mycompany.com/em` as the WebLogic administration user. Then perform the following steps:

1. Locate and select the **Oracle Identity Federation** instance under Identity and Access.

2. Navigate to **Administration**, then **Federations**.

3. Under Trusted Providers, click **Add** to add the Trusted Provider.

4. On the Add Trusted Provider page:

   a. Select **Load Metadata**.

   b. Click **Choose File** and select the SP and IdP metadata files generated in Section 17.3.4.1, "Generating Provider Metadata."

5. On the Federations page, verify that both the providers appear in the list of Trusted Providers.

17.3.4.3 Setting the Default Identity Provider

Proceed as follows to set the Identity Provider registered in the previous section as the default IdP.

Log in to Oracle Enterprise Manager Fusion Middleware Control at `http://admin.mycompany.com/em`

as the WebLogic administration user. Then perform the following steps:

1. Locate and select the **Oracle Identity Federation** instance under Identity and Access.

2. Navigate to **Administration**, then **Service Provider**.

3. For the Default SSO Identity Provider, select the IdP registered above from the list. The Default SSO Identity Provider is under the Protocol Settings section.

17.3.4.4 Updating the Default Authentication Engine to LDAP Engine

When testing integration with Oracle Access Manager in the SP Mode, you cannot configure Oracle Identity Federation as both the Service Provider and Identity Provider for the same resource at the same time. When you test the SP mode configuration, you must set the Default Authentication Engine to the LDAP Engine. You reset it to the Oracle Access Manager once the testing is complete.

This step is not required when configuring the Oracle Identity Federation instances to protect a resource only in the SP mode or in the IdP mode.

To set the Default Authentication Engine, log in to Oracle Enterprise Manager Fusion Middleware Control at `http://admin.mycompany.com/em` as the WebLogic administration user. Then perform the following steps:

1. Locate and select the Oracle Identity Federation instance under Identity and Access.

2. Navigate to **Administration**, then **Authentication Engines**.

3. Select **LDAP Directory** as the Default Authentication Engine from the list.

4. Click **Apply** to save the changes.

17.3.4.5 Updating the Default SSO Response Binding

By default, the Default SSO Response Binding is set to use the SOAP protocol. For ease of testing, Oracle recommends updating this parameter to HTTP POST.

To set the Default SSO Response Binding, log in to Oracle Enterprise Manager Fusion Middleware Control at http://admin.mycompany.com/em as the WebLogic administration user. Then perform the following steps:

1. Navigate to **Administration**, then **Service Provider**.

2. On the Service Provider page, select the **SAML 2.0** tab.

3. Change the value for **Default SSO Response Binding** to **HTTP POST**. The **Default SSO Response Binding** is under the Protocol Settings section.

4. Click **Apply** to save the changes.

17.3.4.6 Validating SP Mode Configuration

Follow these steps to validate the SP mode configuration

1. Using a browser, access the protected resource created in Section 17.3.2.2, "Creating a Resource in Oracle Access Manager," for example: `https://sso.mycompany.com/sso.html`.

2. Enter the credentials of the `weblogic_idm` user on the Login page.

> **Note:** This user must have an email address in the `mail` attribute of the LDAP user record, because the email address is the default `NameID` format used.

3. The protected resource is displayed.

17.3.4.7 Updating the Default Authentication Engine to Oracle Access Manager

In Section 17.3.4.4, "Updating the Default Authentication Engine to LDAP Engine," you set the Default Authentication Engine to LDAP Engine for validating the SP Mode configuration. You must set it back to Oracle Access Manager.

This step is not required when the Oracle Identity Federation instances are configured to protect a resource only in the SP mode or in the IdP mode.

To set the Default Authentication Engine, log in to the Oracle Enterprise Manager Fusion Middleware Control at http://admin.mycompany.com/em as the WebLogic administration user. Then perform the following steps:

1. Locate and select the Oracle Identity Federation instance under Identity and Access.

2. Navigate to **Administration**, then **Authentication Engines**.

3. Select **Oracle Access Manager** as the Default Authentication Engine from the list.

4. Click **Apply** to save the changes.

17.3.4.8 Validating Authentication Mode Configuration

Follow these steps to validate the Authentication mode configuration:

1. Access the Test SP SSO page at: `https://sso.mycompany.com/fed/user/testspsso`

2. Make the following selections on the Initiate Federation SSO page:

   a. Set the value for the **IdP Provider ID** from the list, for example: **Default**

   b. Set the value for **Authn Request Binding** to **HTTP POST** from the list.

   c. Select **Use Default Configuration**.

3. Click Start SSO.

4. Enter the credentials of the `weblogic_idm` user on the Oracle Access Manager login page.

5. The Federation SSO Operation Result page is displayed. Validate that the SSO Authentication Result is successful for the user.

17.4 Auditing Identity 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 17–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 17–1 Audit Event Flow
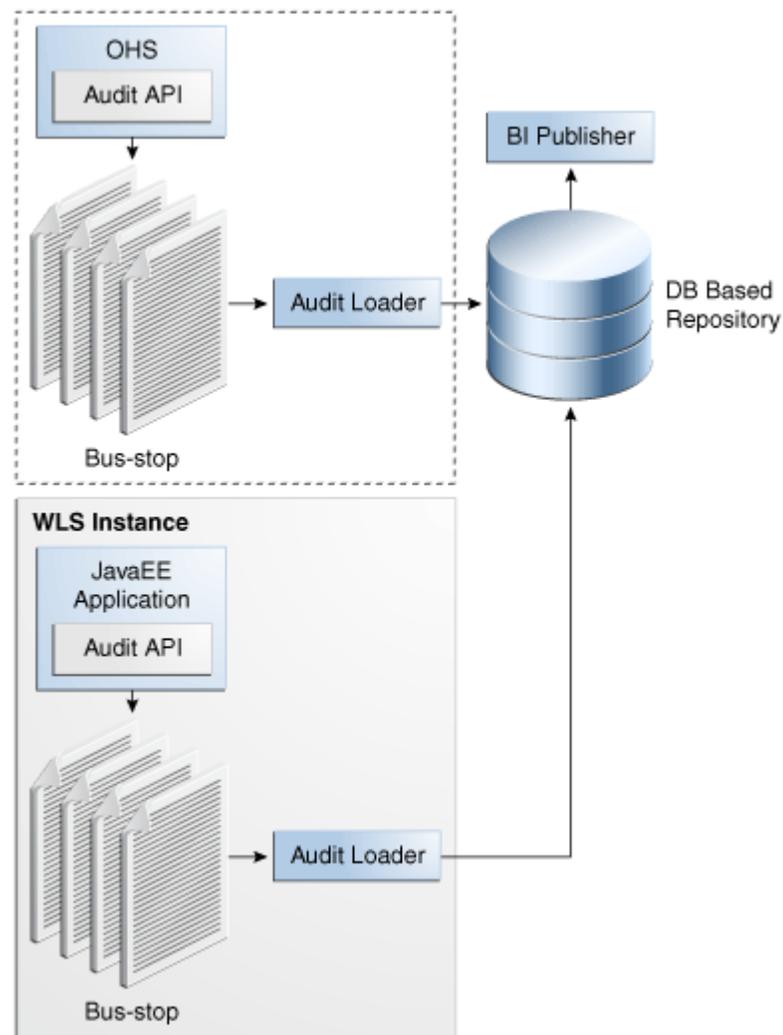
The Oracle Fusion Middleware Audit Framework consists of the following key components:

- 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.

18

Configuring Single Sign-on for Administration Consoles

This chapter describes how to configure single sign-on (SSO) for administration consoles. The administration consoles referred to in the chapter title are:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console
- Oracle Access Manager Console
- Oracle Identity Manager Console

This chapter includes the following topics:

18.1 Configuring Single Sign-On for Administration Consoles with Oracle Access Manager 11g

This section describes how to integrate administration consoles with single sign-on.

This section contains the following topics:

- Section 18.1.1, "Prerequisites"

> **Note:**   Once you have enabled single sign-on for the administration consoles, ensure that at least one Oracle Access Manager server is running to enable console access.
>
> If you have used the Oracle Weblogic console to shut down all of the Oracle Access Manager Managed Servers, then restart one of those Managed Servers manually before using the console again.
>
> To start `WLS_OAM1` manually, use the command:
>
> `DOMAIN_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001`

18.1.1 Prerequisites

Before you attempt to integrate administration consoles with single sign-on, ensure Ensure that the following tasks have been performed:

1. Configure Oracle HTTP Server, as described in Chapter 5, "Configuring the Web Tier."

2. Configure Oracle Access Manager, as described in Chapter 12, "Extending the Domain with Oracle Access Manager 11g."

3. Weblogic Administrators have been provisioned in LDAP as described in Chapter 11.4.4, "Creating Users and Groups for Oracle WebLogic Server."

18.2 Assigning IDM Administrators Group to Weblogic Administration Groups

In an enterprise, it is typical to have a centralized Identity Management domain where all users, groups and roles are provisioned and multiple application domains (such as a SOA domain and WebCenter domain). The application domains are configured to authenticate using the central Identity Management domain.

In Section 11.4.4, "Creating Users and Groups for Oracle WebLogic Server" you created a user called `weblogic_idm` and assigned it to the group IDM Administrators. To be able to manage WebLogic using this account you must add the IDM administrators group to the list of Weblogic Administration groups. This section describes how to add the IDM Administrators Group to the list of WebLogic Administrators.

1. Log in to the WebLogic Administration Server Console.

2. In the left pane of the console, click **Security Realms**.

3. On the Summary of Security Realms page, click **myrealm** under the **Realms** table.

4. On the Settings page for `myrealm`, click the **Roles & Policies** tab.

5. On the Realm Roles page, expand the **Global Roles** entry under the **Roles** table. This brings up the entry for Roles. Click the **Roles** link to go to the Global Roles page.

6. On the Global Roles page, click the **Admin** role to go to the Edit Global Role page:

   a. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.

   b. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.

   c. On the Edit Arguments Page, Specify **IDM Administrators** in the **Group Argument** field and click **Add**.

7. Click **Finish** to return to the Edit Global Rule page.

8. The **Role Conditions** table now shows the `IDM Administrators Group` as an entry.

9. Click **Save** to finish adding the Admin role to the `IDM Administrators Group`.

10. Validate that the changes were successful by bringing up the WebLogic Administration Server Console using a web browser. Log in using the credentials for the `weblogic_idm` user.

18.3 Updating the boot.properties File

The `boot.properties` file for the Administration Server and the Managed Servers should be updated with the WebLogic `admin` user created in Oracle Internet Directory. Follow these steps to update the `boot.properties` file.

For the Administration Server on IDMHOST1

1. On IDMHOST1, go the following directory:

   ORACLE_BASE/admin/domainName/aserver/*domainName*/servers/serverName/security

   For example:

   cd *ORACLE_BASE*/admin/*IDMDomain*/aserver/*IDMDomain*/servers/AdminServer/security

2. Rename the existing `boot.properties` file.

3. Use a text editor to create a file called boot.properties under the security directory. Enter the following lines in the file:

   username=*adminUser*
   password=*adminUserPassword*

   For example:

   username=weblogic_idm
   password=*Password for weblogic_idm user*

   > **Note:** When you start the Administration Server, the username and password entries in the file get encrypted.
   >
   > For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

Restarting the Servers

Restart WebLogic Administration Server and all Managed Servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

18.4 Restarting Servers

Restart the following servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

- Access Servers on `OAMHOST1` and `OAMHOST2`
- Oracle HTTP Servers on `WEBHOST1` and `WEBHOST2`

18.5 Installing and Configuring WebGate

This section describes how to install and configure WebGate. This task is not necessary for OIM11g/OAM10g integration.

This section contains the following topics:

- Section 18.5.1, "Prerequisites"
- Section 18.5.2, "Making Special gcc Libraries Available"

- Section 18.5.3, "Installing Oracle WebGate on WEBHOST1 and WEBHOST2"
- Section 18.5.4, "Patching the Oracle Access Manager 10g WebGates"
- Section 18.5.5, "Validating WebGate"
- Section 18.5.6, "Validating the Oracle Access Manager Single Sign-On Setup"

18.5.1 Prerequisites

Ensure that the following tasks have been performed before installing the Oracle Web Gate:

1. Install and configure the Oracle Web Tier as described in Chapter 5.

2. On Linux systems, make the special versions of the `gcc` libraries available, as described in Chapter 18.

3. Ensure Oracle Access Manager has been configured as described in Chapter 12.

18.5.2 Making Special gcc Libraries Available

Oracle Web Gate requires special versions of `gcc` libraries to be installed (Linux only). These library files must exist somewhere on the Linux system. The Web Gate installer asks for the location of these library files at install time. Download the libraries from `http://gcc.gnu.org`, as described in "Installing Third-Party GCC Libraries (Linux and Solaris Operating Systems Only)" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

> **See Also:**
> `http://www.oracle.com/technetwork/middleware/ias/dow`
> `nloads/10gr3-webgates-integrations-readme-154689.pdf`
> for additional information.

18.5.3 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before you install Oracle WebGate, ensure that the Managed Servers WLS_OAM1 and WLS_OAM2 are started.

Install Oracle WebGate as described in the following sections.

18.5.3.1 Oracle WebGate 10g

Start the Web Gate installer by issuing the command:

```
Oracle_Access_Managerversion_linux_OHS11g_WebGate -gui
```

Then perform the following steps:

1. On the Welcome to the InstallShield Wizard for Oracle Access Manager WebGate screen.

    Click **Next**.

2. On the Customer Information screen, enter the `username` and `group` that the Access Server uses. This should be the same as the user and group that installed the Oracle HTTP Server. The default value for `username` and `group` is `nobody`. For example, enter `oracle/oinstall`.

    Click **Next**.

3. Specify the installation directory for Oracle Access Manager Access Server. For example, enter: *MW_HOME*/oam/webgate.

   Click **Next**.

   > **Note:** Oracle Access Manager WebGate is installed in the access subdirectory under:
   >
   > /u01/app/oracle/product/fmw/oam/webgate.

4. Oracle Access Manager WebGate is installed in:
   /u01/app/oracle/product/fmw/oam/webgate/

   The access directory is created by the installer automatically.

5. Specify the location of the GCC run-time libraries, for example:
   /u01/app/oracle/oam_lib

   Click **Next**.

6. The installation progress screen is shown. After the installation process completes, the WebGate Configuration screen appears.

7. On the WebGate Configuration screen, you are prompted for the transport security mode:

   ```
   The transport security between all Access System components
   (Policy Manager, Access Servers, and associated WebGates)
   must match; select one of the following: Open Mode, Simple
   Mode, or Cert Mode.
   ```

   Select **Simple Mode**.

   Click **Next**.

8. On the next WebGate Configuration screen, specify the following WebGate details:

   - **WebGate ID**: The agent name used in Section 12.6.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool," for example Webgate_IDM.

   - **Password for Web Gate**: If you entered a password when creating the agent, enter this here. Otherwise leave blank.

   - **Access Server ID**: WLS_OAM1

   - **Host Name**: Enter the Host name for one of the Access Servers for example IDMHOST1

   - **Global Access Protocol Passphase**: If your OAM servers are using the Simple security transport protocol, then specify the global passphrase that you use to interact with them.

   - **Port Number the Access Server listens to**: *ProxyPort*

> **Note:** To find the port that the Access Server is using, log in to the oamconsole at:
>
> `http://admin.mycompany.com/oamconsole`
>
> Then perform the following steps:
>
> 1. Select the **System Configuration** tab.
> 2. Select **Server Instances**.
> 3. Select Instance (`WLS_OAM1`) and click the **View** icon in the tool bar.
>
> The proxy entry has host and port information.

9. On the Configure Web Server screen, click **Yes** to automatically update the web server, then click **Next**.

10. On the next Configure Web Server screen, specify the full path of the directory containing the `httpd.conf` file. The `httpd.conf` file is located under the following directory:

    `/u01/app/oracle/admin/`*`ohsInstance`*`/config/OHS/`*`ohsComponentName`*

    For example:

    `/u01/app/oracle/admin/ohs_`
    `instance2/config/OHS/ohs2/httpd.conf`

    Click Next.

11. On the next Configure Web Server page, a message informs you that the Web Server configuration has been modified for WebGate.

    Click **Next**.

12. The next screen, Configure Web Server, displays the following message:

    ```
    If the web server is setup in SSL mode, then httpd.conf file needs to be
    configured with the SSL related parameters. To manually tune your SSL
    configuration, please follow the instructions that come up.
    ```

    Click **Next**.

13. The next screen, Configure Web Server, displays a message with the location of the document that has information on the rest of the product setup, as well as Web Server configuration.

    Select **No** and click **Next**.

14. The final Configure Web Server screen appears with a message to manually launch a browser and open the HTML document for further information on configuring your Web Server.

    Click **Next**.

15. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next**.

16. A message appears, along with the details of the installation, informing you that the installation was successful.

    Click **Finish**.

17. Replace the file `ObAccessClient.xml` in the directory *`MW_`*
    `HOME``/oam/webgate/access/oblix/lib` with the file generated in

Section 12.6.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool."

18. Restart the web server by following the instructions in Chapter 19.1, "Starting and Stopping Oracle Identity Management Components."

19. Repeat for `WEBHOST2`

18.5.3.2 Copying Logout Page to OHS Servers

You must create a logout page to enable applications to log out. A default page exists, but you must edit it and copy it to the WebGate installation on `WEBHOST1` and `WEBHOST2`.

1. Copy the file `logout.html` from the directory *DOMAIN_HOME*`/output/Webgate_IDM` on `IDMHOST1` to *MW_HOME*`/oam/webgate/access/oamsso` on `WEBHOST1` and `WEBHOST2`.

2. Now that you have your own logout page on the web server, you must remove the default entry.

   Edit the file `httpd.conf`, located in the directory:

   ORACLE_INSTANCE`/config/OHS/component name/`

   Comment out the following lines by adding a # at the beginning. The edited lines look like this:

   ```
   #*******Default Login page alias***
   Alias /oamsso "/u01/app/oracle/product/fmw/webgate/access/oamsso"

   #<LocationMatch "/oamsso/*">
   #Satisfy any
   #</LocationMatch>
   #*********************************
   ```

   Save the file.

3. Restart the Oracle HTTP server, as described in Chapter 19.1, "Starting and Stopping Oracle Identity Management Components."

18.5.4 Patching the Oracle Access Manager 10*g* WebGates

This software cannot be patched until it is installed, as described in Section 18.5.3, "Installing Oracle WebGate on WEBHOST1 and WEBHOST2."

Follow these steps to patch the WebGates in your environment:

1. Download the Oracle Access Manager OHS11*g* WebGate patch from My Oracle Support at `https://support.oracle.com`. For 32-bit Linux, the patch name is `Oracle_Access_Manager10_1_4_3_0_BPxx_Patch_linux_OHS11g_WebGate.zip`. For 64-bit Linux it is `Oracle_Access_Manager10_1_4_3_0_BPFA2_Patch_linux64_OHS11g_WebGate.zip`

2. Stop the Oracle HTTP Server 11*g* instances on `WEBHOST1` and `WEBHOST2` by following the steps in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

3. Unzip the `Oracle_Access_Manager10_1_4_3_0_BPxx_Patch_linux_OHS11g_WebGate.zip` file to a temporary location. This creates t two directories. On 32-bit Linux, the directories are:

- `Oracle_Access_Manager10_1_4_3_0_BPxx_Patch_linux_OHS11g_
  WebGate_binary_parameter`

- `Oracle_Access_Manager10_1_4_3_0_BPxx_Patch_linux_OHS11g_
  WebGate_message_en-us`

On 64-bit Linux, the directories are:

- `Oracle_Access_Manager10_1_4_3_0_BPFA2_Patch_linux64_
  OHS11g_WebGate_binary_parameter`

- `Oracle_Access_Manager10_1_4_3_0_BPFA2_Patch_linux64_
  OHS11g_WebGate_message_en-us`

4. Change directory to: *PatchExtractLocation*`/Oracle_Access_Manager10_
   1_4_3_0_BPxx_Patch_linux_OHS11g_WebGate_binary_parameter`

5. Uninstall any existing patches because you must apply patches to the base version.

   To detect the presence of an existing patch, determine the version number, as follows:

   1. Open the file, *webgate-install*`/oblix/config/np1014_wg.txt`

   2. Check the `Version` field.

   If the `Version` value is the base version, 10.1.4.3.0 M11, then it does not contain any patch.

   If the `Version` value is different from the base version, indicating that there is a patch, uninstall the patch as follows:

   a. Navigate to the location within the WebGate installation where the `patchinst` script is present, for example:

   ```
   cd
   /u01/app/oracle/product/fmw/oam/webgate/access/oblix/patch/10143005BP05/Ora
   cle_Access_Manager10_1_4_3_0_BP05_Patch_linux64_OHS11g_WebGate_binary_
   parameter/
   ```

   b. Execute the command:

   ```
   ./patchinst -u
   ```

   c. Specify the WebGate installation area when prompted.

6. Start the patch installation tool by typing:

   ```
   ./patchinst -i InstallDir/access
   ```

   where *InstallDir* is the path to the Access Server install location. For example:

   ```
   /u01/app/oracle/product/fmw/oam/webgate/access
   ```

   This applies the required patch for Oracle Access Manager-Oracle Identity Manager integration to the Oracle Access Manager 10.1.4.3.0 WebGate Instance. Please see the "Enterprise Deployment Guide" chapter of the 11*g* Release 1 (11.1.1) Release Notes for the exact patch level required.

7. Apply this patch to all the WebGate instances in your environment.

8. Start the Oracle HTTP Server instances on `WEBHOST1` and `WEBHOST2`, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

18.5.5 Validating WebGate

You can test that WebGate is functioning correctly by accessing the URL:

`http://admin.mycompany.com/oamconsole`

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

18.5.6 Validating the Oracle Access Manager Single Sign-On Setup

To validate the setup, open a web browser and go the following URLs:

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

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

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

19

Managing Enterprise Deployments

This chapter provides information about managing the Identity Management enterprise deployment you have set up.

This chapter includes the following topics:

19.1 Starting and Stopping Oracle Identity Management Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Identity Management.

This section contains the following topics:

19.1.1 Startup Order

When starting up your entire infrastructure, start the components in the following order:

1. Database(s)
2. Database Listener(s)
3. Oracle Internet Directory
4. Oracle Virtual Directory
5. Access Server(s)
6. WebLogic Administration Server
7. Oracle HTTP Server(s)
8. SOA Server(s)
9. Oracle Identity Manager Server(s)

19.1.2 Starting and Stopping Oracle Virtual Directory

Start and stop Oracle Virtual Directory as follows.

19.1.2.1 Starting Oracle Virtual Directory

Start system components such as Oracle Virtual Directory by typing:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

19.1.2.2 Stopping Oracle Virtual Directory

Stop system components such as Oracle Virtual Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

19.1.3 Starting and Stopping Oracle Internet Directory

Start and stop Oracle Internet Directory as follows.

19.1.3.1 Starting Oracle Internet Directory

Start system components such as Oracle Internet Directory by typing

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

19.1.3.2 Stopping Oracle Internet Directory

Stop system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

19.1.4 Starting, Stopping, and Restarting Oracle HTTP Server

Prior to starting/stopping the Oracle HTTP server ensure that the environment variables `ORACLE_HOME` and `ORACLE_INSTANCE` are defined and that *ORACLE_HOME*/opmn/bin appears in the `PATH`. For example:

```
export WEB_ORACLE_HOME=/u01/app/oracle/product/fmw/web
export ORACLE_INSTANCE=/u01/app/oracle/admin/web[1-2]
export PATH=$ORACLE_HOME/opmn/bin:$PATH
```

19.1.4.1 Starting Oracle HTTP Server

Start the Oracle web tier by issuing the command:

```
opmnctl startall
```

19.1.4.2 Stopping Oracle HTTP Server

Stop the web tier by issuing the command

```
opmnctl stopall
```

to stop the entire Web tier or

```
opmnctl stoproc process-type=OHS
```

to stop Oracle HTTP Server only.

19.1.4.3 Restarting Oracle HTTP Server

You can restart the web tier by issuing a `Stop` followed by a `Start` as described in the previous sections.

To restart the Oracle HTTP server only, use the following command.

```
opmnctl restartproc process-type=OHS
```

19.1.5 Starting and Stopping Node Manager

Start and stop the Node Manager as follows:

19.1.5.1 Starting Node Manager

If the Node Manager being started is the one that controls the Administration Server (`IDMHOST1` or `IDMHOST2`), then prior to starting the Node Manager issue the command:

```
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
```

To start Node Manager, issue the commands:

```
IDMHOST> cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
IDMHOST> ./startNodeManager.sh
```

19.1.5.2 Stopping Node Manager

To stop Node Manager, kill the process started in the previous section.

19.1.5.3 Starting Node Manager for an Administration Server

```
IDMHOST1> cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
IDMHOST1> export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
IDMHOST1> ./startNodeManager.sh
```

> **Note:** It is important to set
> `-DDomainRegistrationEnabled=true` whenever you start a
> Node Manager that manages the Administration Server.

19.1.6 Starting, Stopping, and Restarting WebLogic Administration Server

Start and stop the WebLogic Administration Server as follows:

19.1.6.1 Starting WebLogic Administration Server

The recommended way to start the Administration server is to use WLST and connect
to Node Manager:

```
IDMHOST1> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
IDMHOST1> ./wlst.sh
```

Once in `wlst` shell, execute

```
wls:/offline> nmConnect('Admin_User','Admin_Password','ADMINHOST1','5556',
    'IDMDomain','/u01/app/oracle/admin/domain_name/aserver/IDMDomain')
wls:/nm/domain_name> nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

19.1.6.2 Stopping WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console using the URL:
`http://admin.mycompany.com/console`.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **AdminServer(admin)**.

4. Click **Shutdown** and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shut down the Administration
    Server.

19.1.6.3 Restarting WebLogic Administration Server

Restart the server by following the `Stop` and `Start` procedures in the previous
sections.

19.1.7 Starting, Stopping, and Restarting Oracle Identity Manager

Start and stop Oracle Identity Manager and Oracle SOA Suite servers as follows:

19.1.7.1 Starting Oracle Identity Manager

To start the Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com/console`.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **SOA Servers (WLS_SOA1 and/or WLS_SOA2)**.

> **Note:** You can start the Oracle Identity Manager and Oracle SOA Suite servers independently of each other. There is no dependency in their start order. However, the SOA server must be up and running for all of the Oracle Identity Manager functionality to be available.

4. Click the **Start** button.

5. Click **Yes** when asked to confirm that you want to start the server(s).

6. After WLS_SOA1 and/or WLS_SOA2 have started, select WLS_OIM1 and/or WLS_OIM2

7. Click **Start**.

8. Click **Yes** when asked to confirm that you want to start the server(s).

19.1.7.2 Stopping Oracle Identity Manager

To stop the Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com/console`. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **OIM Servers (WLS_OIM1 and/or WLS_OIM2)** and **(WLS_SOA1 and/or WLS_SOA2)**.

4. Click the **Shutdown** button and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shutdown the server(s).

19.1.7.3 Restarting Oracle Identity Manager

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

19.1.8 Starting, Stopping, and Restarting Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as follows:

19.1.8.1 Starting Oracle Access Manager Managed Servers

To start the Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com/console`.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.

4. Click the **Start** button.

5. Click **Yes** when asked to confirm that you want to start the server(s).

19.1.8.2 Stopping Oracle Access Manager Managed Servers

To stop the Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com/console`. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.

2. Click the **Control** tab.

3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.

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).

19.1.8.3 Restarting Oracle Access Manager Managed Servers

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

19.1.9 Starting and Stopping Oracle Identity Federation Managed Servers

Start and stop Oracle Identity Federation Managed Servers as follows:

19.1.9.1 Starting Oracle Identity Federation

To start the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://admin.mycompany.com/console`. Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.

2. Click the **Control** tab.

3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.

4. Click **Start**.

5. Click **Yes** when asked to confirm that you want to start the server(s).

19.1.9.2 Stopping Oracle Identity Federation

To stop the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at: `http://admin.mycompany.com/console`. Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.

2. Click the **Control** tab.

3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.

4. Click **Shutdown** and select **Force Shutdown now**.

5. Click **Yes** when asked to confirm that you want to shut down the server(s).

19.1.9.3 Restarting Oracle Identity Federation

Restart the server by following the previous Stop and Start procedures.

19.1.9.4 Starting the Oracle Identity Federation Instances and EMAgent

Start the Oracle Identity Federation Instance and EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the instance started successfully by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

19.1.9.5 Stopping the Oracle Identity Federation Instances and EMAgent

Stop the Oracle Identity Federation Instance and EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

19.2 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 19.2.1, "Monitoring Oracle Internet Directory"
- Section 19.2.2, "Monitoring Oracle Virtual Directory"
- Section 19.2.3, "Monitoring Oracle Directory Integration Platform"
- Section 19.2.4, "Monitoring WebLogic Managed Servers"

19.2.1 Monitoring Oracle Internet Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Internet Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.

2. The Identity and Access section below the chart includes the name of each individual Oracle Internet Directory instance, for example, oid1, oid2), its status, host name, and CPU usage percentage. A green arrow in the Status column indicates that the instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Internet Directory instance to view the home page for that instance.

3. The home page for an instance displays metrics for the instance such as performance, load, security, response, CPU utilization %, and memory utilization %.

19.2.1.1 Oracle Internet Directory Component Names Assigned by Oracle Identity Manager Installer

When you perform an Oracle Internet Directory installation using Oracle Identity Management 11*g* Installer, the default component name that the installer assigns to the Oracle Internet Directory instance is oid1. You cannot change this component name.

The instance specific configuration entry for this Oracle Internet Directory instance is `cn=oid1, cn=osdldapd, cn=subconfigsubentry`.

If you perform a second Oracle Internet Directory installation on another computer and that Oracle Internet Directory instance uses the same database as the first instance, the installer detects the previously installed Oracle Internet Directory instance on the other computer using the same Oracle database, so it gives the second Oracle Internet Directory instance a component name of `oid2`.

The instance specific configuration entry for the second Oracle Internet Directory instance is `cn=oid2, cn=osdldapd, cn=subconfigsubentry`. A change of properties in the entry `cn=oid2, cn=osdldapd, cn=subconfigsubentry` does not affect the first instance (`oid1`).

If a third Oracle Internet Directory installation is performed on another computer and that instance uses the same database as the first two instances, the installer gives the third Oracle Internet Directory instance a component name of oid3, and so on for additional instances on different hosts that use the same database.

Note that the shared configuration for all Oracle Internet Directory instances is `cn=dsaconfig, cn=configsets,cn=oracle internet directory`. A change in this entry affects all the instances of Oracle Internet Directory.

This naming scheme helps alleviate confusion when you view your domain using Oracle Enterprise Manager by giving different component names to your Oracle Internet Directory instances.

19.2.2 Monitoring Oracle Virtual Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Virtual Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.

2. The Identity and Access section below the chart includes the name of each instance of the Oracle Virtual Directory application (for example, ovd1, ovd2), its status, and host name. A green arrow in the Status column indicates that the Oracle Virtual Directory instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Virtual Directory instance to view the home page for that instance.

3. The home page for an instance displays metrics and configurations for the instance such as:

   - Oracle Virtual Directory status - A green arrow next to the Oracle Virtual Directory instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.

   - Current Load - This indicates the current work load of this Oracle Virtual Directory instance. It includes three metrics: Open Connections, Distinct Connected Users, and Distinct Connected IP Addresses.

   - Average Response Time Metric - This displays the average time (in milliseconds) to complete an LDAP search request.

   - Operations Metric - This displays the average number of LDAP search requests finished per millisecond.

   - Listeners - This table lists the listeners configured for this Oracle Virtual Directory instance to provide services to clients.

- Adapters - This table lists existing adapters configured with the Oracle Virtual Directory instance. Oracle Virtual Directory uses adapters to connect to different underlying data repositories.

- Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the system resources consumed by the Oracle Virtual Directory instance.

19.2.3 Monitoring Oracle Directory Integration Platform

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Directory Integration Platform, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.

2. The Identity and Access section below the chart includes the name of each instance of the Oracle Directory Integration Platform application (all have the name DIP (11.1.1.1.0)), its status, and host name. Each Oracle Directory Integration Platform instance is deployed in a different Managed Server). A green arrow in the Status column indicates that the Oracle Directory Integration Platform instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Directory Integration Platform instance to view the home page for that instance.

3. The home page for an instance displays metrics for the instance such as:

   - Oracle Directory Integration Platform status - A green arrow next to the Oracle Directory Integration Platform instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.

   - DIP Component Status - This table includes these metrics:

     - Quartz Scheduler - This indicates whether tasks can be scheduled for synchronization or not. A green arrow indicates the scheduler is up and a red arrow indicates that the scheduler is down.

     - Mbeans - This indicates whether profile management is available to the user or not. A green arrow indicates profile management is available and a red arrow indicates profile management is unavailable.

   - Synchronization Profiles - This shows registered profiles and their execution status. In a high availability deployment, all the instances shows the same list of profiles.

   - Provisioning Profiles- This shows registered provisioning profiles and their execution status. In a high availability deployment, all the instances shows the same list of profiles.

   - Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the resource usage by the Oracle Directory Integration Platform instance.

19.2.4 Monitoring WebLogic Managed Servers

You can use Oracle Enterprise Manager Fusion Middleware Control to monitor Managed Servers and other Fusion Middleware components, such as Oracle Access Manager, Oracle Identity Manager, SOA, and Oracle Identity Federation. For more

information, see the administrator guides listed in the Preface under "Related Documents" on page xvii.

19.3 Scaling Enterprise Deployments

The reference enterprise topology discussed in this manual is highly scalable. It can be scaled up and or scaled out. When the topology is scaled up, a new server instance is added to a node already running one or more server instances. When the topology is scaled out, new servers are added to new nodes.

This section contains the following topics:

- Section 19.3.1, "Scaling Up the Topology"
- Section 19.3.2, "Scaling Out the Topology"

19.3.1 Scaling Up the Topology

The Oracle Identity Management topology described in the guide has three tiers: the directory tier, application tier and web tier. The components in all the three tiers can be scaled up by adding a new server instance to a node that already has one or more server instances running.

The procedures described in this section show you how to create a new managed server or directory instance. If you add a new managed server, 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.

For example if you add a new Oracle Access Manager server, you must update `oam.conf` to include the new managed server.

Update `oam.conf` as follows:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
4100
</Location>
```

Once you have updated `oam.conf`, restart the Oracle HTTP server(s) as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components." Oracle recommends that you do this sequentially to prevent loss of service.

19.3.1.1 Scaling Up the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled up on one or both the nodes.

19.3.1.1.1 Scaling Up Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Internet Directory instance.

To add a new Oracle Internet Directory instance to either Oracle Internet Directory node, follow the steps in Section 7.3.2, "Configuring an Additional Oracle Internet Directory Instance" with the following variations:

1. In step 2 and step 4, choose ports other than 389 and 636 since these ports are being used by the existing Oracle Internet Directory instance on the node.

2. Follow the steps in Section 7.4.1, "Registering Oracle Internet Directory with the WebLogic Server Domain" to register the new Oracle Internet Directory instance with the WebLogic domain. Use the location for the new Oracle Internet Directory instance as the value for ORACLE_INSTANCE.

3. Configure SSL server-authentication mode for the new instance as described in Section 7.4.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections."

4. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

5. If you have enabled Single Sign-on in the topology, you must update the WebTier configuration for Single Sign-on as described in Section 18.5, "Installing and Configuring WebGate."

6. Register the new Oracle HTTP Server instance as described in Section 6.10, "Registering Oracle HTTP Server with WebLogic Server."

19.3.1.1.2 Scaling Up Oracle Virtual Directory The directory tier has two nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Virtual Directory instance.

To add a new Oracle Virtual Directory instance to either Oracle Virtual Directory node, follow the steps in Section 9.3.2, "Configuring an Additional Oracle Virtual Directory" with the following variations:

1. In step 2 and step 4, choose ports other than 6501 and 7501 since these ports are being used by the existing Oracle Virtual Directory instance on the node.

2. Follow the steps in these sections to register the new Oracle Virtual Directory instance with the WebLogic domain. Use the location for the new Oracle Virtual Directory instance as the value for ORACLE_INSTANCE.

   - Section 9.4, "Post-Configuration Steps"

   - Section 9.6, "Validating the Oracle Virtual Directory Instances"

   - Section 9.7, "Creating ODSM Connections to Oracle Virtual Directory"

   - Section 9.8, "Creating Adapters in Oracle Virtual Directory"

   - Section 11.4.7, "Updating Oracle Virtual Directory Adapters"

3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

19.3.1.2 Scaling Up the Application Tier

The application tier consists of several nodes in pairs, depending on the products installed. These application servers run either Oracle Directory Services (OID/OVD), Oracle HTTP Servers or WebLogic Managed servers.

Some of the procedures described in this section show you how 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.

For example if you add a new Oracle Access Manager server, you must update `oam.conf` to include the new managed server.

Update `oam.conf` as follows:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
4100
</Location>
```

Once you have updated `oam.conf`, restart the Oracle HTTP server(s) as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components." Oracle recommends that you do this sequentially to prevent loss of service.

19.3.1.2.1 Scaling Up Oracle Directory Integration Platform and ODSM The application tier already has a node (IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager components. The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management Home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for the Oracle Oracle Directory Integration Platform and Oracle Directory Services Manager components.

1. Follow the steps in Section 8.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster".

2. Be sure to choose a port other than 7499, which is already in use.

3. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in Chapter 5, "Configuring the Web Tier" to complete this task.

19.3.1.2.2 Scaling Up Oracle Access Manager 11g Scale up Oracle Access Manager as follows:

Log in to the Oracle WebLogic Server Administration Console at `http://admin.mycompany.com/console`.

1. 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.

2. Click **Lock & Edit** from the Change Center menu.

3. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.

4. Click **Clone**.

5. 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.

6. Click **OK**.

7. Click the newly created server **WLS_OAM3**

8. Click **Save**.

9. 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 `OAMHOSTn`.

   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**.

10. Click **Activate configuration** from the Change Center menu.

Register the new Managed Server with Oracle Access Manager. You now must configure the new Managed Server now as an Oracle Access Manager server. You do this from the Oracle OAM console. Proceed as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.

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 Oracle Access Manager proxy to run on. This is unique for the host
   - **Proxy Server ID**: `AccessServerConfigProxy`
   - **Mode**: Set to `Open` or `Simple`, depending on the mode your existing Oracle Access Manager servers are operating in.

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 19.1, "Starting and Stopping Oracle Identity Management Components."

Add the newly created access server to all WebGate Profiles that might be using it, such as `Webgate_IDM` and `IAMSuiteAgent`

For example, to add the Access server to `Webgate_IDM`, access the OAM console at `http://admin.mycompany.com/oamconsole`, then proceed as follows:

1. Log in as the Oracle Access Manager Admin User you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager."

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** drop down list.

9. Set **Max Connections** to 4.

10. Click **Apply**.

Repeat Steps 5 through 10 for **IAMSuiteAgent** and all other WebGates that might be in use.

Update the Web Tier. Once the new Managed Server has been created and started, the web tier starts to direct requests to it. Best practice, however, is to inform the web server that the new Managed Server has been created.

You do this by updating the file `OAM.conf` on each of the web tiers. This file resides in the directory: *ORACLE_INSTANCE*/config/OHS/*component name*/moduleconf.

Add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>

<Location /fusion_apps>
SetHandler weblogic-handler
WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost1.mycompany.com:1
4101
</Location>

<Location /fusion_apps>
SetHandler weblogic-handler
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
```

```
4100
</Location>
```

Save the file and restart the Oracle HTTP server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

You can now start the new Managed Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

19.3.1.2.3 Scaling Up Oracle Identity Manager (Adding Managed Servers to Existing Nodes) In this case, you already have a node that runs a Managed Server configured with SOA components. The node contains a Middleware home, an Oracle home (SOA) and a domain directory for existing Managed Servers.

You can use the existing installations (the Middleware home, and domain directories) for creating new `WLS_OIM` and `WLS_SOA` servers. There is no need to install the Oracle Identity Manager and Oracle SOA Suite binaries in a new location, or to run pack and unpack.

Follow these steps for scaling up the topology:

1. Using the Administration Console, clone either the `WLS_OIM1` or the `WLS_SOA1` into a new Managed Server. The source Managed Server to clone should be one that already exists on the node where you want to run the new Managed Server.

   To clone a Managed Server:

   a. Select **Environment** -> **Servers** from the Administration Console.

   b. From the Change Center menu, click **Lock and Edit**.

   c. Select the Managed Server that you want to clone (for example, `WLS_OIM1` or `WLS_SOA1`).

   d. Select **Clone**.

   Name the new Managed Server `WLS_OIM`n or `WLS_SOA`n, where n is a number to identify the new Managed Server.

   The rest of the steps assume that you are adding a new server to `OIMHOST1`, which is already running `WLS_SOA1` and `WLS_OIM1`.

2. For the listen address, assign the host name or IP address to use for this new Managed Server. If you are planning to use server migration as recommended for this server, this should be the VIP (also called a floating IP) to enable it to move to another node. The VIP should be different from the one used by the Managed Server that is already running.

3. Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server.

   a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMSServer and name it, for example, `SOAJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage, as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

   Note: This directory must exist before the Managed Server is started or the start operation fails.

   `ORACLE_BASE`/admin/DOMAIN_NAME/cluster_name/jms/SOAJMSFileStore_N

b. Create a new JMS server for SOA, for example, `SOAJMSServer_auto_N`. Use the `SOAJMSFileStore_N` for this JMSServer. Target the `SOAJMSServer_auto_N` server to the recently created Managed Server (`WLS_SOAn`).

c. Create a new JMS server for BPM, for example, `BPMJMSServer_auto_N`. Use the `BPMJMSServer_auto_N` for this JMSServer. Target the `BPMJMSServer_auto_N` server to the recently created Managed Server `WLS_SOAn`.

d. Create a new persistence store for the new BPMJMSServer for example, `BPMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage, as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

e. Create a new persistence store for the new `UMSJMSServer`, for example, `UMSJMSFileStore_N` Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

`ORACLE_BASE`/admin/domain_name/cluster_name/jms/UMSJMSFileStore_N.

> **Note:** This directory must exist before the Managed Server is started or the start operation fails. You can also assign `SOAJMSFileStore_N` as store for the new UMS JMS servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

f. Create a new JMS Server for UMS, for example, `UMSJMSServer_N`. Use the `UMSJMSFileStore_N` for this JMSServer. Target the `UMSJMSServer_N` server to the recently created Managed Server (`WLS_SOAn`).

g. Create a new persistence store for the new OIMJMSServer, for example, `OIMJMSFileStore_N` Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

`ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSFileStore_N`

> **Note:** This directory must exist before the Managed Server is started or the start operation fails. You can also assign `SOAJMSFileStore_N` as store for the new Oracle Identity Manager JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

h. Create a new JMS Server for Oracle Identity Manager, for example, `OIMJMSServer_N`. Use the `OIMJMSFileStore_N` for this JMSServer. Target the `OIMJMSServer_N` server to the recently created Managed Server (`WLS_OIMn`).

i. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for

SOAJMSModule appears. Click the **SubDeployments** tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of `SOAJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `SOAJMSServerXXXXXX` subdeployment. Add the new JMS Server for SOA called `SOAJMSServer_N` to this subdeployment. Click `Save`.

j. Update the SubDeployment targets for the UMSJMSSystemResource to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for UMSJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for UMSJMS appears.

Note: This subdeployment module name is a random name in the form of `UCMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `UMSJMSServerXXXXXX` subdeployment. Add the new JMS Server for UMS called `UMSJMSServer_N` to this subdeployment. Click **Save**.

k. Update the SubDeployment targets for the BPMJMSSystemResource to include the recently created BPM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **BPMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for BPMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for BPMJMS appears.

Note: This subdeployment module name is a random name in the form of `BPMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the **BPMJMSServer*XXXXXX*** subdeployment. Add the new JMS Server for BPM called BPMJMSServer_N to this subdeployment. Click Save.

l. Update the SubDeployment targets for OIMJMSModule to include the recently created Oracle Identity Manager JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSModule** (represented as a hyperlink in the Names column of the table). The Settings page for OIMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for OIMJMS appears.

> **Note:** This subdeployment module name is a random name in the form of `OIMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_OIM1` and `WLS_OIM2`).

Click the `OIMJMSServerXXXXXX` subdeployment. Add the new JMS Server for Oracle Identity Manager called `OIMJMSServer_N` to this subdeployment. Click **Save**.

4. Configure Oracle Coherence, as described in Section 13.6.1, "Updating the Coherence Configuration for the SOA Managed Server."

5. 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 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.

6. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOAn` 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 `SOAHOSTn`. 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_SOAn** 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**.

7. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIMn` Managed Servers. In Step d, select **WLS_OIMn** in the Names column of the table.

8. Click **Activate Changes** from the Change Center menu.

9. Update the SOA host and port using Oracle Enterprise Manager Fusion Middleware Control. Follow these steps:

   a. Open a browser and go to Oracle Enterprise Manager Fusion Middleware Control at: `http://admin.mycompany.com/em`

   b. Log in to Oracle Enterprise Manager Fusion Middleware Control using the Admin user credentials.

> **Note:** At least one of the Oracle Identity Manager Managed Servers must be running for when these steps are executed.

    c. Navigate to **Identity and Access**, and then **oim**.

    d. Right-click **oim** and navigate to **System MBean Browser**.

    e. Under **Application Defined MBeans**, navigate to **oracle.iam**, **Application:oim**, **XMLConfig**, **Config**, **XMLConfig.SOAConfig**, and then **SOAConfig**.

    f. Update the value for the **Rmiurl** attribute with the host and port of the new SOA server. Click **Apply** to save the changes.

    g. The **Rmiurl** attribute is used for accessing SOA EJBs deployed on SOA Managed Servers. This is the application server URL. For a clustered deployment of Oracle Identity Manager, it is a comma-delimited list of all the SOA Managed Server URLs. The following are example values for this attribute:

```
t3://oimhost1.mycompany.com:8001,oimhost2.mycompany.com:80
01,oimhost3.mycompany.com:8001
```

10. Restart the WebLogic Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

11. 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.

12. Configure the newly created managed server for server migration. Follow the steps in Section 16.5, "Configuring Server Migration Targets" to configure server migration.

13. 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.

19.3.1.3 Scaling Up Oracle Identity Federation

The application tier already has a node (`OIFHOST2`) running a Managed Server configured with Oracle Identity Federation. The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for Oracle Identity Federation.

1. Follow the steps in Section 14.3, "Configuring Oracle Identity Federation on OIFHOST2" to scale up the topology for Oracle Identity Federation.

2. Be sure to choose a port other than 7499, which is already in use.

3. Follow the steps in Section 14.4, "Provisioning the Managed Servers on the Local Disk" to provision the new Oracle Identity Federation managed server on the local disk.

4. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in Chapter 5, "Configuring the Web Tier," to complete this task.

19.3.1.4 Scaling Up 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 up the Oracle HTTP Server, follow the steps in Chapter 5, "Configuring the Web Tier."

1. Use the Oracle Fusion Middleware 11*g* Web Tier Utilities Configuration Wizard to scale up the topology, as described in Chapter 5, "Configuring the Web Tier."

2. Copy all files created in *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf from the existing web tier configuration to the new one.

3. Register the new Oracle HTTP Server instance, as described in Section 6.10, "Registering Oracle HTTP Server with WebLogic Server."

4. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

19.3.2 Scaling Out the Topology

In scaling out a topology, new servers are added to new nodes. The components in all three tiers of the Oracle Identity Management topology described in this manual can be scaled out by adding a new server instance to a new node.

19.3.2.1 Scaling Out the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled out by adding new nodes to the directory tier.

19.3.2.1.1 Scaling Out Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The Oracle Internet Directory instances can be scaled out by

adding a new node to the existing Oracle Internet Directory cluster. To scale out Oracle Internet Directory instances, follow these steps:

1. Follow the steps in Section 7.3.2, "Configuring an Additional Oracle Internet Directory Instance" to add a new node running Oracle Internet Directory.

2. Follow the steps in Section 7.4.1, "Registering Oracle Internet Directory with the WebLogic Server Domain" to register the new Oracle Internet Directory instance with the WebLogic domain.

3. Configure SSL server authentication mode for the new instance, as described in Section 7.4.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections."

4. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

19.3.2.1.2 Scaling Out Oracle Virtual Directory The directory tier has two nodes (`OVDHOST1` and `OVDHOST2`), each running an Oracle Virtual Directory instance. Oracle Virtual Directory can be scaled out by adding a new node configured to run Oracle Virtual Directory to the directory tier. To scale out Oracle Virtual Directory instances, follow these steps:

1. Follow the steps in Section 9.3.2, "Configuring an Additional Oracle Virtual Directory" to add a new node running Oracle Virtual Directory.

2. Follow the steps in these sections to register the new Oracle Virtual Directory instance with the WebLogic domain.

   - Section 9.4, "Post-Configuration Steps"

   - Section 9.6, "Validating the Oracle Virtual Directory Instances"

   - Section 9.7, "Creating ODSM Connections to Oracle Virtual Directory"

   - Section 9.8, "Creating Adapters in Oracle Virtual Directory"

   - Section 11.4.7, "Updating Oracle Virtual Directory Adapters"

3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

19.3.2.2 Scaling Out the Application Tier

The application tier has two nodes (`IDMHOST1` and `IDMHOST2`) running Managed Servers for Oracle Directory Integration Platform and Oracle Directory Services Manager, and two nodes (`OAMHOST1` and `OAMHOST2`) running the Oracle Access Manager Access Server.

Some of the procedures described in this section show you how 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.

For example if you add a new Oracle Access Manager server, you must update `oam.conf` to include the new managed server.

Update `oam.conf` as follows:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
4100
```

```
</Location>
```

Once you have updated `oam.conf`, restart the Oracle HTTP server(s) as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components." Oracle recommends that you do this sequentially to prevent loss of service.

19.3.2.2.1 Scaling Out Oracle Identity Federation The application tier has two nodes (`OIFHOST1` and `OIFHOST2`) running a Managed Server configured with Oracle Identity Federation. The Oracle Identity Federation instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

To scale out the Oracle Identity Federation instances, follow these steps:

1. Follow the steps in these sections to scale out the Oracle Identity Federation instances in the topology.

   - Section 14.3, "Configuring Oracle Identity Federation on OIFHOST2"

   - Section 14.4, "Provisioning the Managed Servers on the Local Disk"

   - Section 14.5, "Validating Oracle Identity Federation"

   - Section 14.6, "Configure the Enterprise Manager Agents"

2. Follow the steps in Section 14.8, "Configuring Oracle Identity Federation to work with the Oracle Web Tier" to add the newly added Managed Server host name and port to the list WebLogicCluster parameter.

19.3.2.2.2 Scaling Out Oracle Directory Integration Platform and ODSM The application tier has two nodes (IDMHOST1 and IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager. The Oracle Directory Integration Platform and Oracle Directory Services Manager instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

To scale out DIP and ODSM instances, follow these steps:

1. Follow the steps in Section 8.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster" to scale out the Oracle Directory Integration Platform and Oracle Directory Services Manager instances in the topology.

2. Reconfigure the Oracle HTTP Server module with the new Managed Server.

   Follow the steps in Section 8.4, "Configuring ODSM to work with the Oracle Web Tier." for the instructions to complete this task.

   Add the newly added Managed Server host name and port to the list WebLogicCluster Parameter.

19.3.2.2.3 Scaling Out Oracle Access Manager 11g Scale out is very similar to scale up but first requires the software to be installed on the new node.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

> **Note:** If you are using shared storage, allow the new host access to that shared storage area.

1. On the new node, mount the existing Middleware home, which should include the SOA 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.

2. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME`/bea/beahomelist file and add `ORACLE_BASE`/product/fmw to it.

3. Log in to the Oracle WebLogic Server Administration Console at `http://admin.mycompany.com/console`.

4. 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.

5. Click **Lock & Edit** from the Change Center menu.

6. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.

7. Click **Clone**.

8. 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.

9. Click **OK**.

10. Click the newly created server **WLS_OAM3**.

11. Set the SSL listen port. This should be unique on the host that the Managed Server runs on.

12. Click **Save**.

13. 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 `IDMHOSTn`.

    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 was propagated to the cloned server. To disable host name verification, proceed as follows:

    a. In Oracle Enterprise Manager Fusion Middleware Control, select Oracle WebLogic Server Administration Console.

    b. Expand the **Environment** node in the Domain Structure pane.

    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**.

14. Click **Activate Configuration** from the Change Center menu.

15. Restart the WebLogic Administration Server as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

16. Pack the domain on IDMHOST1 using the command:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/tmp/IDMDomain.jar -template_name="OAM Domain" -managed=true
```

The pack.sh script is located in *MW_HOME*/oracle_common/common/bin.

17. Unpack the domain on the new host using the command:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain
-template=/tmp/IDMDomain.jar -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

The unpack.sh script is located in *MW_HOME*/oracle_common/common/bin.

18. Start Node Manager and update the property file.

    a. Start and stop Node Manager as described in Section 19.1, "Starting and Stopping Oracle Identity Management 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 19.1, "Starting and Stopping Oracle Identity Management Components."

Register the new Managed Server with Oracle Access Manager. The new Managed Server now must be configured as an Oracle Access Manager server. You do this from the Oracle OAM console, as follows:

1. Log in to the OAM console at http://admin.mycompany.com/oamconsole as the oamadmin user.

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 is running on, IDMHOST3.

    ▪ **Port**: Listen port that was assigned when the Managed Server was created.

- **OAM Proxy Port**: Port you want the Oracle Access Manager proxy to run on. This is unique for the host.

- **Proxy Server ID:** `AccessServerConfigProxy`

- **Mode**: Set to `Open` or `Simple`, depending on the mode your existing Oracle Access Manager servers are operating in.

6. Click **Apply**.

Add the newly created access server to all WebGate profiles that might be using it, such as `Webgate_IDM` and `IAMSuiteAgent`.

For example, to add the Oracle Access Manager server to Webgate_IDM, access the OAM console at `http://admin.mycompany.com/oamconsole` and proceed as follows:

1. Log in as the Oracle Access Manager admin user you created in Section 11.4.2, "Creating Users and Groups for Oracle Access Manager."

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** drop down list.

9. Set **Max Connections** to `4`.

10. Click **Apply**

Repeat Steps 5 through 10 for `IAMSuiteAgent` and other WebGates that are in use.

Update the Web Tier. Now that the new Managed Server has been created and started, the web tier starts to direct requests to it. Best practice, however, is to inform the web server that the new Managed Server has been created.

You do this by updating the file `OAM.conf` on each of the web tiers. This file resides in the directory: `ORACLE_INSTANCE/config/OHS/component name/moduleconf`.

Add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>

<Location /fusion_apps>
SetHandler weblogic-handler
WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
SetHandler weblogic-handler
```

```
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
4100
</Location>

<Location /fusion_apps>
SetHandler weblogic-handler
WebLogicCluster
idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100,idmhost3.mycompany.com:1
4100
</Location>
```

19.3.2.2.4 Scaling Out Oracle Identity Manager (Adding Managed Servers to New Nodes) When you scale out the topology, you add new Managed Servers configured with SOA to new nodes.

Before performing the steps in this section, check that you meet these requirements:

- There must be existing nodes running Managed Servers configured with SOA within the topology.

- The new node can access the existing home directories for WebLogic Server and SOA.

  Use the existing installations in shared storage for creating a new WLS_SOA or WLS_OIM Managed Server. You do not need to install WebLogic Server or SOA binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

Notes:

- If there is no existing installation in shared storage, installing WebLogic Server and SOA in the new nodes is required as described in Section 13.6.1, "Updating the Coherence Configuration for the SOA Managed Server."

- When an `ORACLE_HOME` or `WL_HOME` is shared by multiple servers in different nodes, Oracle recommends keeping the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the oraInventory in a node and attach an installation in a shared storage to it, use:

  `ORACLE_HOME`/oui/bin/attachHome.sh

- To update the Middleware home list to add or remove a WL_HOME, edit the `user_home`/bea/beahomelist file. See the following steps.

Follow these steps for scaling out the topology:

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.

2. To attach `ORACLE_HOME` in shared storage to the local Oracle Inventory, execute the following command:

   ```
   SOAHOSTn> cd ORACLE_BASE/product/fmw/soa/oui/bin
   SOAHOSTn> ./attachHome.sh -jreLoc JAVA_HOME
   ```

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *MW_HOME*/bea/beahomelist file and add *ORACLE_BASE*/product/fmw to it.

4. Log in to the Oracle WebLogic Administration Console.

5. Create a new machine for the new node to be used, and add the machine to the domain.

6. Update the machine's Node Manager's address to map the IP address of the node that is being used for scale out.

7. Use the Oracle WebLogic Server Administration Console to clone WLS_SOA1 into a new Managed Server. Name it WLS_SOA*n*, where *n* is a number.

> **Note:** These steps assume that you are adding a new server to node *n*, where no Managed Server was running previously.

8. Assign the host name or IP address to use for the new Managed Server for the listen address of the Managed Server.

9. If you are planning to use server migration for this server (which Oracle recommends) this should be the VIP address (also called a floating IP address) for the server. This VIP address should be different from the one used for the existing Managed Server.

10. Create JMS servers for SOA, Oracle Identity Manager (if applicable), and UMS on the new Managed Server.

   a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMSServer and name it, for example, SOAJMSFileStore_*N*. Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure." For example:

   ORACLE_BASE/admin/domain_name/cluster_
   name/jms/SOAJMSFileStore_*N*

   > **Note:** This directory must exist before the Managed Server is started or the start operation fails.

   b. Create a new JMS Server for SOA, for example, SOAJMSServer_auto_*N*. Use the SOAJMSFileStore_*N* for this JMSServer. Target the SOAJMSServer_auto_*N* Server to the recently created Managed Server (WLS_SOA*n*).

   c. Create a new persistence store for the new UMSJMSServer, and name it, for example, UMSJMSFileStore_*N*. Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

   ORACLE_BASE/admin/domain_name/cluster_
   name/jms/UMSJMSFileStore_*N*

Notes:

- This directory must exist before the Managed Server is started or the start operation fails.

- It is also possible to assign `SOAJMSFileStore_N` as the store for the new UMS JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

---

d. Create a new JMS server for UMS: for example, `UMSJMSServer_N`. Use the `UMSJMSFileStore_N` for this JMS server. Target the `UMSJMSServer_N` server to the recently created Managed Server (`WLS_SOAn`).

e. Create a new persistence store for the new BPMJMSServer, and name it, for example, `BPMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

ORACLE_BASE/admin/domain_name/cluster_ name/jms/BPMJMSFileStore_*N*

Notes:

- This directory must exist before the Managed Server is started. Otherwise, the start operation fails.

- It is also possible to assign `SOAJMSFileStore_N` as the store for the new BPM JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

---

f. Create a new JMS server for BPM, for example, `BPMJMSServer_N`. Use the `BPMJMSFileStore_N` for this JMS server. Target the `BPMJMSServer_N` server to the recently created Managed Server (`WLS_SOAn`).

g. Create a new persistence store for the new `OIMJMSServer`, and name it, for example, `OIMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in Section 2.4, "Shared Storage and Recommended Directory Structure."

ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSFileStore_*N*

Notes:

- This directory must exist before the Managed Server is started or the start operation fails.

- It is also possible to assign `SOAJMSFileStore_N` as the store for the new Oracle Identity Manager JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

---

h. Create a new JMS Server for Oracle Identity Manager: for example, `OIMJMSServer_N`. Use the `OIMJMSFileStore_N` for this JMS Server. Target

the `OIMJMSServer_N`Server to the recently created Managed Server (`WLS_OIMn`).

i. Update the SubDeployment targets for the BPMJMSSystemResource to include the recently created BPM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **BPMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for BPMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for BPMJMS appears.

Note: This subdeployment module name is a random name in the form of `BPMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `BPMJMSServerXXXXXX` subdeployment. Add the new JMS Server for BPM called `BPMJMSServer_N` to this subdeployment. Click **Save**.

j. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for **SOAJMSModule** appears. Open the SubDeployments tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of `SOAJMSServer` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `SOAJMSServerXXXXXX` subdeployment. Add the new JMS Server for SOA called `SOAJMSServer_N` to this subdeployment. Click **Save**.

k. Update the SubDeployment targets for UMSJMSSystemResource to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the **Names** column of the table). The Settings page for `UMSJMSSystemResource` appears. Open the **SubDeployments** tab. The subdeployment module for `UMSJMS` appears

---

Note: This subdeployment module is a random name in the form of `UMSJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `UMSJMSServerXXXXXX` subdeployment. Add the new JMS Server for UMS called `UMSJMSServer_N` to this subdeployment. Click **Save**.

l. Update the SubDeployment Targets for `OIMJMSModule` to include the recently created Oracle Identity Manager JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose JMS Modules from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSModule** (represented as a hyperlink in the Names column of the table). The Settings page for `OIMJMSModule` appears. Click the **SubDeployments** tab. The subdeployment module for `OIMJMS` appears.

> **Note:** This subdeployment module is a random name in the form of `OIMJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `OIMJMSXXXXXX` subdeployment. Add the new JMS Server for Oracle Identity Manager called `OIMJMSServer_N` to this subdeployment. Click **Save**.

11. Click **Activate Configuration** from the Change Center menu.

12. Run the `pack` command on `SOAHOST1` to create a template pack as follows:

```
Prompt> cd ORACLE_COMMON_HOME/common/bin
Prompt> ./pack.sh -managed=true -domain=MW_HOME/user_
projects/domains/soadomain/ -template=soadomaintemplateScale.jar -template_
name=soa_domain_templateScale
```

Run the following command on `SOAHOST1` to copy the template file created to `SOAHOSTN`:

```
Prompt> scp soadomaintemplateScale.jar oracle@SOAHOSTN:/ORACLE_
BASE/product/fmw/soa/common/bin
```

Run the `unpack` command on `SOAHOSTN` to unpack the template in the Managed Server domain directory as follows:

```
SOAHOSTN> cd ORACLE_BASE/product/fmw/soa/common/bin

SOAHOSTN> ./unpack.sh -domain=ORACLE_BASE/product/fmw/user_
projects/domains/soadomain/ -template=soadomaintemplateScale.jar -app_
dir=ORACLE_BASE/admin/IDMDomain/mserver/applications
```

13. Configure Oracle Coherence, as described in Section 13.6.1, "Updating the Coherence Configuration for the SOA Managed Server."

14. Update the SOA host and port using Oracle Enterprise Manager Fusion Middleware Control. Follow these steps:

   a. Open a browser and go to Oracle Enterprise Manager Fusion Middleware Control at:

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

   b. Log in to Oracle Enterprise Manager Fusion Middleware Control using the `admin` user credentials.

   > **Note:** At least one of the Oracle Identity Manager Managed Servers must be running for when these steps are executed.

c. Navigate to **Identity and Access**, and then **oim**.

d. Right-click **oim** and navigate to **System MBean Browser**.

e. Under **Application Defined MBeans**, navigate to **oracle.iam**, **Application:oim**, **XMLConfig**, **Config**, **XMLConfig.SOAConfig**, and then **SOAConfig**.

f. Update the value for the **Rmiurl** attribute with the host and port of the new SOA server. Click **Apply** to save the changes.

g. The **Rmiurl** attribute is used for accessing SOA EJBs deployed on SOA Managed Servers. This is the application server URL. For a clustered deployment of Oracle Identity Manager, it is a comma-delimited list of all the SOA Managed Server URLs. The following are example values for this attribute:

```
t3://oimhost1.mycompany.com:8001

oimhost2.mycompany.com:8001

oimhost3.mycompany.com:8001
```

15. 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 Administration Console, select **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.

16. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOAn` 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 `SOAHOSTn`. 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 setting is propagated to the cloned server).

To disable host name verification:

a. Expand the **Environment** node in the **Domain Structure** window.

b. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.

c. Click **Servers**. The Summary of Servers page appears.

d. Select **WLS_SOAn** 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**.

17. Click **Activate Configuration** from the Change Center menu.

18. Start the Node Manager on the new node. To start the Node Manager, use the installation in shared storage from the existing nodes, and start Node Manager by passing the host name of the new node as a parameter as follows:

```
SOAHOSTN> WL_HOME/server/bin/startNodeManager new_node_ip
```

19. Start and test the new Managed Server from the Oracle WebLogic Server Administration Console:

1. Shut down all the existing Managed Servers in the cluster.

2. Ensure that the newly created Managed Server, `WLS_SOAn`, is running.

3. Access the application on the newly created Managed Server (`http://vip:port/soa-infra`). The application should be functional.

20. Configure server migration for the new Managed Server.

> **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 address for the new SOA Managed Server is already present in the new node.

Configure server migration following these steps:

a. Log in to the Administration Console.

b. In the left pane, expand **Environment** and select **Servers**.

c. Select the server (represented as hyperlink) for which you want to configure migration from the **Names** column of the table. The Setting page for that server appears.

d. Click the **Migration** tab.

e. In the **Available** field, in the **Migration Configuration** section, select the machines to which to enable migration and click the right arrow.

> **Note:** Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional Managed Server.

f. Select the **Automatic Server Migration Enabled** option. This enables the Node Manager to start a failed server on the target node automatically.

g. Click **Save**.

h. Restart the Administration Server, Managed Servers, and Node Manager.

i. Test server migration for this new server. Follow these steps from the node where you added the new server:

1. Abruptly stop the `WLS_SOAn` Managed Server.

2. To do this, run:

```
kill -9 pid
```

on the (PID) of the Managed Server. You can identify the PID of the node using:

```
ps -ef | grep WLS_SOAn
```

3. Watch the Node Manager Console. You should see a message indicating that floating IP address for `WLS_SOA1` has been disabled.

4. Wait for the Node Manager to try a second restart of `WLS_SOAn`. Node Manager waits for a fence period of 30 seconds before trying this restart.

5. 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.

19.3.2.3 Scaling Out the Web Tier

The web tier has two nodes each running an instance of the Oracle HTTP Server. The Oracle HTTP Server components can be scaled out by adding a new node configured to run Oracle HTTP Server to the web tier. To scale out Oracle HTTP Server, proceed as follows:

1. Follow the steps in Section 4.4, "Installing Oracle HTTP Server." Alternatively, on the new node, mount the existing Middleware home, if you are using shared storage.

2. Follow the steps in Chapter 5, "Configuring the Web Tier."

3. Copy all files created in `ORACLE_ INSTANCE`/config/OHS/`component`/moduleconf from the existing web tier configuration to the new one.

4. If you have enabled Single Sign-on in the topology, you must update the WebTier configuration for Single Sign-on as described in Section 18.5, "Installing and Configuring WebGate."

5. Register the new Oracle HTTP Server instance as described in Section 6.10, "Registering Oracle HTTP Server with WebLogic Server."

6. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

19.4 Performing Backups and Recoveries

Table 19–1 shows the static artifacts to back up in the 11*g* Oracle Identity Management enterprise deployment.

Table 19–1   Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier

Oracle Home (database)	Oracle RAC database hosts:
	
	`OIDDBHOST1`
	
	`OIDDBHOST2`
		User Defined	Directory Tier

`MW_HOME` (OID)	`OIDHOST1` `OIDHOST2`	MW_HOME: `/u01/app/oracle/product/fmw` ORACLE HOME: `/u01/app/oracle/product/fmw/idm` on both the OIDHOST1 and OIDHOST2	Directory Tier
`MW_HOME` (OVD)	`OVDHOST1` `OVDHOST2`	MW_HOME: `/u01/app/oracle/product/fmw` ORACLE HOME: `/u01/app/oracle/product/fmw/idm` on both the OVDHOST1 and OVDHOST2	Directory Tier
`MW_HOME` (DIP, ODSM, OIM, OAM11g, OIF and Admin Server)	`IDMHOST1` `IDMHOST2`	FMW_HOME: `/u01/app/oracle/product/fmw` DIP/ODSM ORACLE HOME: `/u01/app/oracle/product/fmw/idm` on both IDMHOST1 and IDMHOST2 ADMIN SERVER ORACLE HOME: `/u01/app/oracle/product/fmw/idm` on both IDMHOST1 and IDMHOST2	Application Tier
`MW_HOME` (OHS)	`WEBHOST1` `WEBHOST2`	MW_HOME: `/u01/app/oracle/product/fmw` ORACLE HOME: `/u01/app/oracle/product/fmw/web` on WEBHOST1 ORACLE HOME: `/u01/app/oracle/product/fmw/web` on WEBHOST2	Web Tier

Install Related Files	Each host	OraInventory:
		`ORACLE_BASE/orainventory`
		`/etc/oratab, /etc/oraInst.loc`
		`user_home/bea/beahomelist` (on hosts where WebLogic Server is installed)
		Windows registry: (HKEY_LOCAL/MACHINE/Oracle)
			Not applicable.

Table 19–2 shows the run-time artifacts to back up in the 11*g* Oracle Identity Management enterprise deployment:

Table 19–2   Run-Time Artifacts to Back Up in the Identity Management Enterprise Deployments

Type	Host	Location	Tier
DOMAIN HOME	`IDMHOST1` `IDMHOST2`	*ORACLE_ BASE*/admin/*IDMDomain*/aserver on both `IDMHOST1` and `IDMHOST2`	Application Tier
Application Artifacts (ear and war files)	`IDMHOST1` `IDMHOST2`	Look at all the deployments, including Oracle Directory Integration Platform and Oracle Directory Services Manager, through the WebLogic Server Administration Console to identity all the application artifacts.	Application Tier

INSTANCE HOME (OHS)	`WEBHOST1`
	`WEBHOST2`
		OHS INSTANCE HOME on `WEBHOST1`:
		
		`/u01/app/oracle/admin/ohs_`
		`inst/oamAdmin_ohs`
			Application Tier

OID INSTANCE HOME	`OIDHOST1`
	`OIDHOST2`
		OID INSTANCE HOME on `OIDHOST1`:
		
		`/u01/app/oracle/admin/oid_inst1`
		OID INSTANCE HOME on `OIDHOST2`:
		
		`/u01/app/oracle/admin/oid_inst2`
			Directory Tier

OVD INSTANCE HOME	`OVDHOST1`
	`OVDHOST2`
		OVD INSTANCE HOME on `OVDHOST1`:
		
		`/u01/app/oracle/admin/ovd_inst1`
		OVD INSTANCE HOME on `OVDHOST2`:
		
		`/u01/app/oracle/admin/ovd_inst2`
			Directory Tier

Oracle RAC Databases	`OIDDBHOST1` `OIDDBHOST2`	User defined	Directory Tier
OAM	`OAMHOST1` `OAMHOST2`	All the configurations are within the respective home directories described in this table. There are no instance homes.	Application Tier

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

19.5 Patching Enterprise Deployments

This section describes how to apply an Oracle Fusion Middleware patch file and how to patch Oracle Identity Management components with minimal down time.

This section contains the following topics:

- Section 19.5.1, "Patching an Oracle Fusion Middleware Source File"

- Section 19.5.2, "Patching Identity Management Components"

19.5.1 Patching an Oracle Fusion Middleware Source File

For information on patching an Oracle Fusion Middleware source file, see the *Oracle Fusion Middleware Administrator's Guide*.

19.5.2 Patching Identity Management Components

To patch Oracle Identity Management components with minimal down time, it is recommended that you follow these guidelines:

1. Route the LDAP traffic from OIDHOST1 and OVDHOST1 to OIDHOST2 and OVDHOST2.

2. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST1 or OVDHOST1).

3. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.

4. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.

5. Test the patch.

6. Route the traffic to OIDHOST1 or OVDHOST1 again.

7. Verify the applications are working properly.

8. Route the LDAP traffic on OIDHOST2 and OVDHOST2 to OIDHOST1 and OVDHOST1.

9. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST2 or OVDHOST2).

10. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.

11. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.

12. Test the patch.

13. Route the traffic to both hosts on which the patch has been applied (OIDHOST1 and OIDHOST2, or OVDHOST1 and OVDHOST2).

19.6 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 19.6.1, "Troubleshooting Oracle Internet Directory"
- Section 19.6.2, "Troubleshooting Oracle Virtual Directory"
- Section 19.6.3, "Troubleshooting Oracle Directory Integration Platform"
- Section 19.6.4, "Troubleshooting Oracle Directory Services Manager"
- Section 19.6.5, "Troubleshooting Oracle Access Manager 11g"
- Section 19.6.6, "Troubleshooting Oracle Identity Manager"
- Section 19.6.7, "Troubleshooting Oracle Identity Federation"

19.6.1 Troubleshooting Oracle Internet Directory

This section describes some common problems that can arise with Oracle Internet Directory and the actions you can take to resolve the problem.

Problem

The Oracle Internet Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Internet Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to Oracle Internet Directory server

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

The LDAP application is receiving LDAP Error 53 (DSA Unwilling to Perform). When one of the database nodes goes down during the middle of the LDAP transaction, the Oracle Internet Directory server sends error 53 to the LDAP client

Solution

To see why the Oracle Internet Directory database node went down, see the Oracle Internet Directory logs in this location:

```
ORACLE_INSTANCE/diagnostics/logs/OID/oidldapd01s*.log
```

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

19.6.2 Troubleshooting Oracle Virtual Directory

This section describes some common problems that can arise with Oracle Virtual Directory and the actions you can take to resolve the problem:

Problem

You get a `command not found` error when you run `SSLServerConfig.sh`, for example:

```
./SSLServerConfig.sh: line 169: 20110520125611: command not found
```

Solution

Edit the file `orapki.bat` (on Windows) or `orapki.sh` (on Linux) and remove any blank lines at the end of the file. Save the file and run `SSLServerConfig.sh` again.

Problem

Oracle Virtual Directory is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Virtual Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to the Oracle Virtual Directory server.

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

19.6.3 Troubleshooting Oracle Directory Integration Platform

This section describes some common problems that can arise with Oracle Directory Integration Platform and the actions you can take to resolve the problem.

Problem

The instance is not working properly.

Solution

Check the respective log of the instance. For example, if the instance deployed in WLS_ODS1 is not running, then check the WLS_ODS1-diagnostic.log file.

Problem

Exceptions similar to the following are seen in Managed Server log files running the Oracle Directory Integration Platform application during an Oracle RAC failover:

```
RuntimeException:
[2008-11-21T00:11:10.915-08:00] [WLS_ODS] [ERROR] []
[org.quartz.impl.jdbcjobstore.JobStoreTX] [tid: 25] [userId: <anonymous>]
[ecid: 0000Hqy69UiFW7V6u3FCEH199aj0000009,0] [APP: DIP] ClusterManager: Error
managing cluster: Failed to obtain DB connection from data source
'schedulerDS': java.sql.SQLException: Could not retrieve datasource via JNDI
url 'jdbc/schedulerDS' java.sql.SQLException: Cannot obtain connection:
driverURL = jdbc:weblogic:pool:schedulerDS, props =
{EmulateTwoPhaseCommit=false, connectionPoolID=schedulerDS,
jdbcTxDataSource=true, LoggingLastResource=false,
dataSourceName=schedulerDS}.[[
Nested Exception: java.lang.RuntimeException: Failed to setAutoCommit to true
for pool connection

AuthenticationException while connecting to OID:
[2008-11-21T00:12:08.812-08:00] [WLS_ODS] [ERROR] [DIP-10581] [oracle.dip]
[tid: 11] [userId: <anonymous>] [ecid: 0000Hqy6m54FW7V6u3FCEH199apO0000000,0]
[APP: DIP] DIP was not able to get the context with the given details {0}[[
javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid
Credentials]
```

Most of the exceptions are related to the scheduler or LDAP, for example:

1. Could not retrieve datasource via JNDI url 'jdbc/schedulerDS'
java.sql.SQLException.

2. javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]

Solution

During an Oracle RAC failover, exceptions are seen in the Managed Server log files running the Oracle Directory Integration Platform application. These errors are thrown when the multi data sources configured on the WebLogic Server platform try to verify the health of the Oracle RAC database instances during failover. These are innocuous errors and can be ignored. The Oracle Directory Integration Platform application recovers and begin to operate normally after a lag of one or two minutes. For an Oracle RAC failover, there is no Oracle Directory Integration Platform down time if one instance is running at all times.

19.6.4 Troubleshooting Oracle Directory Services Manager

This section describes some common problems that can arise with Oracle Directory Services Manager and the actions you can take to resolve the problem.

After you have logged into Oracle Directory Services Manager, you can connect to multiple directory instances from the same browser window.

Avoid using multiple windows of the same browser program to connect to different directories at the same time. Doing so can cause a Target unreachable error.

You can log in to the same Oracle Directory Services Manager instance from different browser programs, such as Internet Explorer and Firefox, and connect each to a different directory instance.

If you change the browser language setting, you must update the session to use the new setting. To update the session, either disconnect the current server connection, refresh the browser page (either reenter the Oracle Directory Services Manager URL in the URL filed and press enter or press F5) and reconnect to the same server, or quit and restart the browser.

Problem

You attempt to invoke Oracle Directory Services Manager from Oracle Enterprise Manager Fusion Middleware Control by selecting Directory Services Manager from the Oracle Internet Directory menu in the Oracle Internet Directory target, then Data Browser, Schema, Security, or Advanced.

Oracle Directory Services Manager does not open. You might see an error message.

Solution

This is probably an installation problem. See Oracle Fusion Middleware Installation Guide for Oracle Identity Management.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.

2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.

3. Make a connection to an Oracle Internet Directory server.

4. Work with the Oracle Internet Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.

5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.

6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Internet Directory.

7. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.

2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.

3. Re-establish a new connection to the Oracle Internet Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to Oracle Internet Directory and displays the message LDAP Server is down.

Solution

In a High Availability configuration where Oracle Directory Services Manager is connected to Oracle Internet Directory through a load balancer, Oracle Directory Services Manager reports that the server is down during failover from one instance of Oracle Internet Directory to another. In other configurations, this message might indicate that Oracle Internet Directory has been shut down and restarted. In either case, the connection is reestablished in less than a minute, and you are able to continue without logging in again.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Internet Directory instance that is using a Oracle RAC database. Oracle Directory Services Manager might display the message

LDAP error code 53 - Function not implemented.

Solution

This error can occur during failover of the Oracle Database that the Oracle Internet Directory instance is using. The connection is reestablished in less than a minute, and you are able to continue without logging in again.

Problem

You must perform the following steps to configure Oracle HTTP Server to route Oracle Directory Services Manager requests to multiple Oracle WebLogic Servers in a clustered Oracle WebLogic Server environment.

Solution

Perform these steps:

1. Create a backup copy of the Oracle HTTP Server's `admin.conf` file, which is located in `ORACLE_INSTANCE`/config. The backup copy provides a source to revert to if you encounter problems after performing this procedure.

2. Add the following text to the end of the Oracle HTTP Server's `admin.conf` file and replace the variable placeholder values with the host names and Managed Server port numbers specific to your environment. Be sure to use the `<Location /odsm/ >` as the first line in the entry. Using `<Location /odsm/faces >` or `<Location /odsm/faces/odsm.jspx >` can distort the appearance of the Oracle Directory Services Manager interface.

```
<Location /odsm/ >
SetHandler weblogic-handler
WebLogicCluster host-name-1:managed-server-port,host-name_2:managed_server_port
</Location>
```

3. Restart the Oracle HTTP Server, as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components," to activate the configuration change.

> **Note:** Oracle Directory Services Manager loses its connection and displays a session time-out message if the Oracle WebLogic Server in the cluster that it is connected to fails. Oracle Directory Services Manager requests is routed to the secondary Oracle WebLogic Server in the cluster that you identified in the httpd.conf file after you log back in to Oracle Directory Services Manager.

Problem

Attempting to access Oracle Directory Services Manager using a web browser fails.

Solution

- Verify the Oracle Virtual Directory server is running. The Oracle Virtual Directory server must be running to connect to it from Oracle Directory Services Manager.

- Verify you entered the correct credentials in the Server, Port, User Name and Password fields. You can execute an ldapbind command against the target Oracle Virtual Directory server to verify the server, user name, and password credentials.

- Verify you are using a supported browser. Oracle Directory Services Manager supports the following browsers:

  - Internet Explorer 7

  - Firefox 2.0.0.2 and 3.0

  - Safari 3.1.2 (desktop)

  - Google Chrome 0.2.149.30

  > **Note:** While Oracle Directory Services Manager supports all of the preceding browsers, only Internet Explorer 7 and Firefox 2.0.0.2 are certified.

Problem

Oracle Directory Services Manager does not open after you attempt to invoke it from Oracle Enterprise Manager Fusion Middleware Control by selecting one of the options from the **Directory Services Manager** entry in the **Oracle Virtual Directory** menu in the Oracle Virtual Directory target.

Solution

This is probably an installation problem. See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.

2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.

3. Make a connection to an Oracle Virtual Directory server.

4. Work with the Oracle Virtual Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.

5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.

6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Virtual Directory. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.

2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.

3. Re-establish a new connection to the Oracle Virtual Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Virtual Directory instance that is using an Oracle RAC Database. Oracle Directory Services Manager might display the message `LDAP error code 53 - Function not implemented`.

Solution

This error can occur during failover of the Oracle Database that the Oracle Virtual Directory instance is using. The connection is reestablished in less than a minute, and you are able to continue without logging in again.

19.6.5 Troubleshooting Oracle Access Manager 11g

This section describes some common problems that can arise with Oracle Access Manager and the actions you can take to resolve the problem.

19.6.5.1 User Reaches the Maximum Allowed Number of Sessions

Problem

The Oracle Access Manager 11*g* 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 OAM Administration Console.

To modify the configuration by using the OAM 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. Specifiying a value of 0 allows each user to have an unlimited number of login sessions.

19.6.5.2 Policies Do Not Get Created When Oracle Access Manager is First Installed

Problem

The Administration Server takes a long time to start after configuring Oracle Access Manager.

Solution

Tune the OAM database. When the Administration server first starts after configuring Oracle 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.

19.6.5.3 You Are Not Prompted for Credentials After Accessing A Protected Resource

Problem

When you access a protected resource, Oracle 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 IDMDomain have been set. You should have aliases for `IDMDomain:80`, `IDMDomain:Null:`, `admin.mycompany.com:80`, and `sso.mycompany.com:443`.

2. Verify that WebGate is installed.

3. Verify that `OBAccessClient.xml` was copied from *DOMAIN_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 Oracle Access Manager when it first starts.

5. Shut down the Oracle Access Manager servers and try to access the protected resource. You should see an error saying Oracle Access Manager servers are not available. If you do not see this error, re-install WebGate.

19.6.6 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.

Problem

If you are creating a user in Oracle Identity Manager (by logging into Oracle Identity Manager, 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.

19.6.7 Troubleshooting Oracle Identity Federation

This section describes some common problems that can arise with Oracle Identity Federation and the actions you can take to resolve the problem.

Problem

On a Windows system, you cannot log in to the Oracle Identity Federation server even though it is running.

Solution

Make sure that the Oracle Identity Federation server is using IPv4, if everything else is using IPv4).

To verify this, look in the file *DOMAIN_HOME*/bin/setDomainEnv.cmd on OIFHOST1 and OIFHOST2.

Locate the line EXTRA_JAVA_PROPERTIES and add the following to the entry if it is not already present:

```
-Djava.net.preferIPv6Addresses -DuseIPv6Address=false
-Djava.net.preferIPv6Addresses=false
```

Save the file and restart the Oracle Identity Federation servers as described in Section 19.1, "Starting and Stopping Oracle Identity Management Components."

Problem

You cannot change Oracle Identity Federation parameters by using Oracle Enterprise Manager Fusion Middleware Control. You see the message:

```
Configuration settings are unavailable because ..... OIF ......
is down
```

even though Oracle Identity Federation is up and running.

Solution

Here are the common causes and resolutions:

1. Oracle Identity Federation is up but the EM agent is down.

   a. Check the EM agent status by running:

      ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl status agent

   b. Start the EM agent, if it is down, by running:

      ORACLE_INSTANCE/bin/opmnctl startproc ias-component=EMAGENT

   c. Log in to Fusion Middleware Control again.

2. Oracle Identity Federation and EM agent are up, but the OIF home page and configuration pages in Fusion Middleware Control still show: **OIF is down**.

a. Check if the EM agent points to the correct Fusion Middleware Control by running:

```
ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl status agent
```

Verify that the `host` and `port` for property `Repository URL` are the same as the Fusion Middleware Control's host and port.

b. If the `host` and `port` are mismatched, change the `Repository URL` in EM agent to the correct Fusion Middleware Control by running:

```
ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl switchOMS
http(s)://Host:Port/em/upload'
```

c. Log in to Fusion Middleware Control again.

3. If the issue still exists, once logged in to Fusion Middleware Control, navigate to **Farm**->**Agent-Monitored Targets** (Top Left corner of the page) and click the **Configure** icon of the row that refers to Oracle Identity Federation. On the next page, ensure that all the information is correct and complete. Click **OK** to confirm.

Check that the WebLogic user name and password are present.

Check the host value. It might have been specified with an IPv6 address format.

4. If the issue still exists, restart the EM agent.

a. Stop the EM agent by running:

```
INST_HOME/bin/opmnctl stopproc ias-component=EMAGENT
```

b. Start the EM agent by running:

```
INST_HOME/bin/opmnctl startproc ias-component=EMAGENT
```

c. Log in to Oracle Enterprise Manager Fusion Middleware Control again.

19.7 Other Recommendations

This section describes some other recommendations for the Oracle Identity Management enterprise deployment.

19.7.1 Preventing Timeouts for SQL*Net Connections

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.

Index