Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.3.0)

E57013-03

December 2017

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

ORACLE

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

E57013-03

Primary Author: Shynitha Shanthakumar

Contributors: Firdaus Fraz, Michael Rhys, Michael Zanchelli, Nagasravani Akula, Peter LaQuerre, Venkateswarlu Karnati

Contents

2 Understanding the IAM Enterprise Deployment

3 Understanding the IAM Exalogic Enterprise Deployment

4 Using the Enterprise Deployment Workbook

5 Procuring Resources for an Enterprise Deployment

6 Preparing the Load Balancer and Firewalls for an Enterprise Deployment

7 Preparing Storage for an Enterprise Deployment

11 Installing Oracle Fusion Middleware in Preparation for an Enterprise Deployment

12 Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment

13 Preparing The Identity Store

14 Configuring the Oracle Web Tier

15 Creating Domains for an Enterprise Deployment

16 Setting Up Node Manager for an Enterprise Deployment

17 Configuring Oracle Access Management

18 Configuring Oracle Mobile Security Services

19 Configuring Oracle Identity Manager

20 Configuring BI Publisher

21 Configuring Server Migration for an Enterprise Deployment

22 Configuring Single Sign-On

23 Introduction to the Life Cycle Management (LCM) Tools

24 Installing Oracle Identity and Access Management Life Cycle Management Tools

25 Creating a Deployment Response File

26 Deploying Identity and Access Management

27 Performing Post-Deployment Configuration

30 Topology Tool Commands for Scaling

31 Managing the Topology for an Enterprise Deployment

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

- *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- *Oracle Database Backup and Recovery User's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide

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

New and Changed Features for 11*g* Release 2 (11.1.2.3)

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3) differs from previous versions in that the majority of the components are configured using the Identity and Access Management Life Cycle Management (LCM) tools.

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

New LDAP Directory Options

EDG now supports both OUD and OID as a backend directory. Note: In an OID scenario only OID is shown. ODSM for OID is outside the scope of this EDG. In addition to OUD and OID, Active Directory is also supported.

New Oracle Identity and Access Management Life Cycle Management Tools

The new Oracle Identity and Access Management Life Cycle Management (LCM) tool (deployment tool) does the following:

- Creates RCU schema objects
- Provisions using a single command.

The Oracle Identity and Access Management Life Cycle Management tool does not create an LDAP directory. If you wish to create an LDAP directory for use by the deployment tool, create it using the manual steps in this guide.

Newly Added Manual Deployment Procedure

The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* 11*g* Release 2 (11.1.2.3) includes manual steps for setting up an enterprise deployment.

New Product Support

The new product support includes the following:

- Oracle Privileged Account Manager
- BI Publisher Light
- Mobile Security Suite (Formally Bitzer)

Deployment Procedure on Exalogic

The standard guide has been enhanced to include the different steps required to deploy Oracle Identity and Access Management on Exalogic. The steps described in this guide are for the Fusion Middleware aspects of the deployment only.

For information on how to configure the Exalogic appliance in preparation for deploying Oracle Fusion Middleware, refer to the *Oracle Fusion Middleware Enterprise Deployment Guide for Exalogic*.

Other New Features

This release of Oracle Identity and Access Management includes the following additional features:

- New Oracle Access Management (OAM) administration architecture.
- Extra Entry point URL for Oracle Mobile Security Suite.
- Inclusion of Oracle Mobile Security Access Server (MSAS) Proxy in the web tier. The MSAS Proxy acts as a security agent in its own right and therefore does not sit behind the Web Server.
- Changes to facilitate Multi Data Center (MDC).
- Separation of Entry point URLs into `login.example.com` and `prov.example.com`. This allows Access Domain to be setup in an active/active Multidata Center configuration, while allowing the governance domain to be Active/Passive.
- Separation of data into two different databases. Oracle Access Management MDC has two open active databases, so having the Access Domain data located in a dedicated database allows this to happen. Having the Governance Domain data (plus OID if used) in a different database allows that database to be protected using Active Dataguard.
- Governance Domain Admin Server moved to OIMHOST2. This means that, on a single host (pair) deployment, the admin servers are distributed across hosts rather than everything being located onto a single host.
- Exadata Virtual - LDAP moved to dedicated vServers to make the topology similar to the platform distributed model.

Part I

Understanding an Enterprise Deployment

Part I contains the following chapters:

1

Understanding a Typical Enterprise Deployment

This chapter describes the general characteristics of a typical Oracle Fusion Middleware enterprise deployment. You can apply the concepts here to any product-specific enterprise deployment.

This chapter contains the following sections:

1.1 Diagram of a Typical Enterprise Deployment

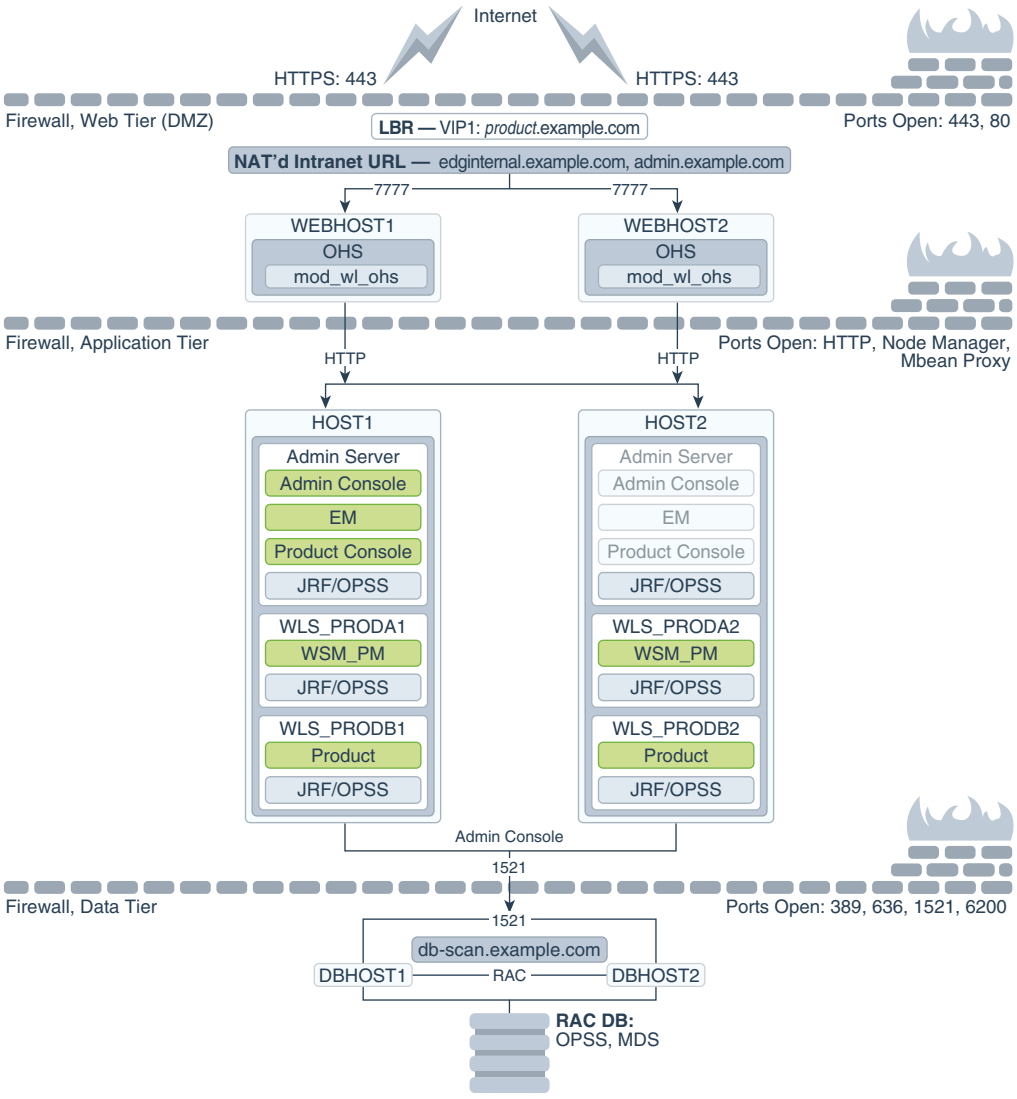
All Oracle Fusion Middleware enterprise deployments are designed to demonstrate the best practices for installing and configuring an Oracle Fusion Middleware production environment.

A best practices approach starts with the basic concept of a multi-tiered deployment and standard communications between the different software tiers.

Figure 1–1 shows a typical enterprise deployment, including the Web tier, application tier and data tier.

For a description of each tier and the standard protocols used for communications within a typical Oracle Fusion Middleware enterprise deployment see Section 1.2, "Understanding the Typical Enterprise Deployment Topology Diagram".

Figure 1–1 Typical Enterprise Deployment Topology Diagram



1.2 Understanding the Typical Enterprise Deployment Topology Diagram

The following sections provide a detailed description of the typical enterprise topology diagram:

- Section 1.2.1, "Understanding the Firewalls and Zones of a Typical Enterprise Deployment"
- Section 1.2.2, "Understanding the Tiers of a Typical Enterprise Deployment Topology"
- Section 1.2.3, "Processing Requests"
- Section 1.2.4, "Understanding Storage"
- Section 1.2.5, "Understanding the Web Tier"
- Section 1.2.6, "Understanding the Application Tier"
- Section 1.2.7, "About the Data Tier"

1.2.1 Understanding the Firewalls and Zones of a Typical Enterprise Deployment

The topology is divided into several security zones, which are separated by firewalls:

The firewalls are configured to allow data to be transferred only through specific communication ports. Those ports (or in some cases, the protocols that will need open ports in the firewall) are shown on each firewall line in the diagram.

For example:

- On the firewall protecting the Web tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.
- On the firewall protecting the Application tier, Oracle WebLogic Server Node manager, HTTP ports, and MBean proxy port are open.

  Applications that require external HTTP access can use the Oracle HTTP Server instances as a proxy. Note that this port for outbound communications only and the proxy capabilities on the Oracle HTTP Server must be enabled.
- On the firewall protecting the Data tier, the database listener port (typically, 1521) must be open.

  The LDAP ports (typically, 389 and 636) are also required to be open for communication between the authorization provider and the LDAP-based identity store.

  The ONS port (typically, 6200) is also required so the application tier can receive notifications about workload and events in the Oracle RAC Database. These events are used by the Oracle WebLogic Server connection pools to adjust quickly (creating or destroying connections), depending on the availability and workload on the Oracle RAC database instances.

For a complete list of the ports you must open for a specific Oracle Fusion Middleware enterprise deployment topology, see the chapter that describes the topology you want to implement, or refer to the *Enterprise Deployment Workbook* for the topology you are implement. For more information, see LINK TO CHAPTER.

1.2.2 Understanding the Tiers of a Typical Enterprise Deployment Topology

The enterprise deployment topology consists of the following high-level tiers:

- A hardware load balancer that routes requests from the Internet to the Web servers in the Web tier. It also routes requests from internal clients or other components that are performing internal invocations within the corporate network.
- A Web tier, consisting of two or more physical computers that are hosting Web server instances (for load balancing and high availability).

  The Web server instances are configured to authenticate users (via an external identity store and a single sign-on server) and then route the HTTP requests to the Oracle Fusion Middleware products and components running in the Application tier.

  The Web server instances also host static Web content that does not require application logic to be delivered. Placing such content in the Web tier reduces the overhead on the application servers and eliminates unnecessary network activity.
- An Application tier, consisting of two or more physical computers that are hosting a cluster of Oracle WebLogic Server Managed Servers, and the Administration Server for the domain. The Managed Servers are configured to run the various Oracle Fusion Middleware products, such as Oracle SOA Suite and Oracle Service Bus.

- A Data tier, consisting of two or more physical hosts that are hosting an Oracle RAC Database.

1.2.3 Processing Requests

In a typical enterprise topology, a hardware load balancer directs incoming HTTP and HTTPS requests from the Internet to the Web tier. In addition, the hardware load balancer routes specific communications between the Oracle Fusion Middleware components and applications on the application tier. The internal-only requests are also routed through the load balancer, using a unique virtual host name. For more information, see the following:

- Section 1.2.3.1, "Purpose of the Hardware Load Balancer (LBR)"
- Section 1.2.3.2, "Summary of the Typical Load Balancer Virtual Server Names"
- Section 1.2.3.3, "HTTPS versus HTTP Requests to the External Virtual Server Name"

1.2.3.1 Purpose of the Hardware Load Balancer (LBR)

The hardware load balancer routes the following types of requests:

- Section 1.2.3.1.1, "Requests from the Internet to the Web server instances in the Web tier"
- Section 1.2.3.1.2, "Specific internal-only communications between the components of the Application tier"

1.2.3.1.1 Requests from the Internet to the Web server instances in the Web tier The hardware load balancer balances the load on the Web tier by receiving requests to a single virtual host name and then routing each request to one of the Web server instances, based on a load balancing algorithm. In this way, the load balancer ensures that no one Web server is overloaded with HTTP requests.

For more information about the purpose of specific virtual host names on the hardware load balancer, see Section 1.2.3.2, "Summary of the Typical Load Balancer Virtual Server Names."

In the reference topology, only HTTP requests are routed from the hardware load balancer to the Web tier. Secure Socket Layer (SSL) requests are terminated at the load balancer and only HTTP requests are forwarded to the Oracle HTTP Server instances. This guide does not provide instructions for SSL configuration between the load balancer and the Oracle HTTP Server instances or between the Web tier and the Application tier.

The load balancer provides high availability by ensuring that if one Web server goes down, requests will be routed to the remaining Web servers that are up and running.

Further, in a typical highly available configuration, two hardware load balancers are configured in an active-passive configuration such that, the passive load balancer acts as a hot standby and is ready to resume service in case a failure occurs in the main load balancing appliance. This is important because for many types of services and systems, the hardware load balancer becomes the unique point of access to make invocations and, as a result, becomes a single point of failure for the whole system if it is not protected.

1.2.3.1.2 Specific internal-only communications between the components of the Application tier In addition, the hardware load balancer routes specific communications between the Oracle Fusion Middleware components and applications on the application tier. The

internal-only requests are also routed through the load balancer, using a unique virtual host name.

1.2.3.2 Summary of the Typical Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, the hardware load balancer is configured to recognize a set of virtual server names. As shown in the diagram, the following virtual server names are recognized by the hardware load balancer in this topology:

- `<product>.example.com` - This virtual server name is used for all incoming traffic.

  Users enter this URL (`http://myapplication.example.com`) to access the Oracle Fusion Middleware products and custom applications available on this server. The load balancer then routes these requests (using a load balancing algorithm) to one of the servers in the Web tier. In this way, the single virtual server name can be used to route traffic to multiple servers for load balancing and high availability of the Web servers instances.

- `edginternal.example.com` - This virtual server name is for internal communications only.

  The load balancer uses its **Network Address Translation (NAT)** capabilities to route any internal communication from the Application tier components that are directed to the `http://edginternal.example.com/` Intranet URL. This URL is not exposed to external customers or users on the Internet.

- `admin.example.com` - This virtual server name is for administrators who need to access the Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server Administration Console interfaces.

  This URL is known only to internal administrators. It also uses the NAT capabilities of the load balancer to route administrators to the active Administration Server in the domain.

For the complete set of virtual server names you must define for your topology, see the chapter that describes the product-specific topology.

1.2.3.3 HTTPS versus HTTP Requests to the External Virtual Server Name

Any request on port 80 (non-SSL protocol) is redirected to port 443 (SSL protocol). Exceptions of this rule include requests from public WSDLs. For more information, see Section 6.1, "Configuring Virtual Hosts on the Hardware Load Balancer."

1.2.4 Understanding Storage

Shared storage is an allocation of disk space that is accessible by all of the subscribers in a network, intended for file storage and allowing simultaneous access by multiple subscribers without the need to duplicate files to their computers. Shared storage is typically delivered from a Storage Area Network (SAN) or a network attached storage server (NAS).

A Disk Volume or Share is an area of a disk which has been allocated on the SAN/NAS, which usually contains a file system. This volume is mounted onto individual host computers as necessary.

If an application uses a number of disk shares then these can be grouped together into a Project or Volume Group. Shares can then be managed on a share by share basis or collectively as part of the project. For example, if your SAN or NAS provides snapshots for backup and recovery, you can snapshot an entire project, allowing you to backup everything to do with an application in a single unit, or you can snapshot it at

the individual share/volume level to provide more precise backups. This could be used as part of a backup strategy for backing up the entire Project each month, or each day, for example, for the share containing configuration information.

Shares can be mounted exclusively or shared.

- If you mount a share exclusively, you are extending the local storage, meaning, it is mounted on only one host at a time and dedicated to it. This is slower than using local disk directly, but does provide the benefit of SAN/NAS backup and recovery.
- Shared mounts are mounted on several hosts, all of which have the ability to write to and read from the share. If you have a shared mount where each host is trying to write to the same file at the same time you may experience issues with service.

1.2.5 Understanding the Web Tier

The Web tier of the reference topology consists of two Oracle HTTP Server instances.

For more information about the Web tier, see the following sections:

- Section 1.2.5.1, "Benefits of Using Oracle HTTP Server Instances to Route Requests"
- Section 1.2.5.2, "Alternatives to Using Oracle HTTP Server in the Web Tier"
- Section 1.2.5.3, "About the WebLogic Proxy Plug-In"

1.2.5.1 Benefits of Using Oracle HTTP Server Instances to Route Requests

A Web tier with Oracle HTTP Server is not a requirement for many of the Oracle Fusion Middleware products. You can route traffic directly from the hardware load balancer to the WLS servers in the Application Tier. However, a Web tier does provide several advantages, which is why it is recommended as part of the reference topology:

- The Web tier provides DMZ public zone, which is a common requirement in security audits. If a load balancer routes directly to the WebLogic Server, requests move from the load balancer to the application tier in one single HTTP jump, which can cause security concerns.
- The Web tier allows the WebLogic Server cluster membership to be reconfigured (new servers added, others removed) without having to change the Web server configuration (as long as at least some of the servers in the configured list remain alive).
- Oracle HTTP Server delivers static content more efficiently and faster than WebLogic Server; it also provides FTP services, which are required for some enterprise deployments, as well as the ability to create virtual hosts and proxies via the Oracle HTTP Server configuration files.
- Oracle HTTP Server provides HTTP redirection over and above what WebLogic Server provides. You can use Oracle HTTP Server as a front end against many different WebLogic Server clusters, and in some cases, control the routing via content based routing.
- Oracle HTTP Server provides the ability to integrate single sign-on capabilities into your enterprise deployment. For example, you can later implement single sign-on for the enterprise deployment, using Oracle Access Manager, which is part of the Oracle Identity and Access Management family of products.
- Oracle HTTP Server provides support for WebSocket connections deployed within WebLogic Server.

- Some deployments, such as those on Exalogic, may use Oracle Traffic Director instead of Oracle HTTP Server.

For more information about Oracle HTTP Server, see "Introduction to Oracle HTTP Server" in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

1.2.5.2 Alternatives to Using Oracle HTTP Server in the Web Tier

Although Oracle HTTP Server provides a variety of benefits in an enterprise topology, Oracle also supports routing requests directly from the hardware load balancer to the Managed Servers in the middle tier.

This approach provide the following advantages:

- Lower configuration and processing overhead than using a front-end Oracle HTTP Server Web tier front-end.
- Monitoring at the application level since the load balancer can be configured to monitor specific URLS for each Managed Server (something that is not possible with OHS).

1.2.5.3 About the WebLogic Proxy Plug-In

As shown in the diagram, the Oracle HTTP Server instances use the WebLogic Proxy Plug-In (`mod_wl_ohs`) to proxy HTTP requests from Oracle HTTP Server to the Oracle WebLogic Server Managed Servers in the Application tier.

For more information, see "Overview of Web Server Proxy Plug-Ins 12.1.3" in *Oracle Fusion Middleware Using Web Server 1.1 Plug-Ins with Oracle WebLogic Server*.

1.2.6 Understanding the Application Tier

The application tier consists of two physical host computers, where Oracle WebLogic Server and the Oracle Fusion Middleware products are installed and configured. The application tier computers reside in the secured zone between firewall 1 and firewall 2.

For more information, see the following sections:

- Section 1.2.6.1, "Configuration of the Administration Server and Managed Servers Domain Directories"
- Section 1.2.6.2, "Best Practices and Variations on the Configuration of the Clusters and Hosts on the Application Tier"
- Section 1.2.6.3, "About the Node Manager Configuration in a Typical Enterprise Deployment"
- Section 1.2.6.4, "About Using Unicast for Communications Within the Application Tier"
- Section 1.2.6.5, "Understanding OPSS and Requests to the Authentication and Authorization Stores"

1.2.6.1 Configuration of the Administration Server and Managed Servers Domain Directories

Unlike the Managed Servers in the domain, the Administration Server uses an active-passive high availability configuration. This is because only one Administration Server can be running within an Oracle WebLogic Server domain.

In the topology diagrams, the Administration Server on HOST1 is in the active state and the Administration Server on HOST2 is in the passive (inactive) state.

To support the manual fail over of the Administration Server in the event of a system failure, the typical enterprise deployment topology includes:

- A Virtual IP Address (VIP) for the routing of Administration Server requests
- The configuration of the Administration Server domain directory on a shared storage device.

In the event of a system failure (for example a failure of HOST1), you can manually reassign the Administration Server VIP address to another host in the domain, mount the Administration Server domain directory on the new host, and then start the Administration Server on the new host.

However, unlike the Administration Server, there is no benefit to storing the Managed Servers on shared storage. In fact, there is a potential performance impact when Managed Server configuration data is not stored on the local disk of the host computer.

As a result, in the typical enterprise deployment, after you configure the Administration Server domain on shared storage, a copy of the domain configuration is placed on the local storage device of each host computer, and the Managed Servers are started from this copy of the domain configuration. You create this copy using the Oracle WebLogic Server pack and unpack utilities.

The resulting configuration consists of separate domain directories on each host: one for the Administration Server (on shared storage) and one for the Managed Servers (on local storage).

For more information about the structure of the Administration Server domain directory and the Managed Server domain directory, as well as the variables used to reference these directories, see Section 7.5.

1.2.6.2 Best Practices and Variations on the Configuration of the Clusters and Hosts on the Application Tier

In a typical enterprise deployment, you configure the Managed Servers in a cluster on two or more hosts in the application tier. For specific Oracle Fusion Middleware products, the enterprise deployment reference topologies demonstrate best practices for the number of Managed Servers, the number of clusters, and what services are targeted to each cluster.

These best practices take into account typical performance, maintenance, and scale-out requirements for each product. The result is the grouping of Managed Servers into an appropriate set of clusters within the domain.

Variations of the enterprise deployment topology allow the targeting of specific products or components to additional clusters or hosts for improved performance and isolation.

For another example, you can host the Administration Server on a separate and smaller host computer, which allows the FMW components and products to be isolated from the Administration Server.

These variations in the topology are supported, but the enterprise deployment reference topology uses the minimum hardware resources while keeping high availability, scalability and security in mind. You should perform the appropriate resource planning and sizing, based on the system requirements for each type of server and the load that the system needs to sustain. Based on these decisions, you must adapt the steps to install and configure these variations accordingly from the instructions presented in this guide.

1.2.6.3 About the Node Manager Configuration in a Typical Enterprise Deployment

In a typical Enterprise Deployment, there is one node manager per host. This node manager can start managed servers from any domain. This is the Node Manager configuration recommended for an Enterprise Deployment.

In a typical enterprise deployment, you configure a Per Domain Node Manager, and you start two Node Manager instances on the Administration Server host: one from the Administration Server domain directory and one from the Managed Servers domain directory.

Starting the Node Manager from each domain directory creates two isolated Node Manager processes that can be used independently to control each type of server. The separate Node Manager processes allow you to use different features for the Administration Server Node Manager and the Managed Servers Node Manager.

1.2.6.4 About Using Unicast for Communications Within the Application Tier

Oracle recommends the unicast communication protocol for communication between the Managed Servers and hosts within the Oracle WebLogic Server clusters in an enterprise deployment. Unlike multicast communication, unicast does not require cross-network configuration and it reduces potential network errors that can occur from multicast address conflicts as well.

When you consider using the multicast or unicast protocol for your own deployment, consider the type of network, the number of members in the cluster, and the reliability requirements for cluster membership. Also consider the following benefits of each protocol.

Benefits of unicast in an enterprise deployment:

- Uses a group leader that every server sends messages directly to. This leader is responsible for retransmitting the message to every other group member and other group leaders, if applicable.
- Works out of the box in most network topologies
- Requires no additional configuration, regardless of the network topology.
- Uses a single missed heartbeat to remove a server from the cluster membership list.

Benefits of multicast in an enterprise deployment:

- Multicast uses a more scalable peer-to-peer model where a server sends each message directly to the network once and the network makes sure that each cluster member receives the message directly from the network.
- Works out of the box in most modern environments where the cluster members are in a single subnet.
- Requires additional configuration in the router(s) and WebLogic Server (i.e., Multicast TTL) if the cluster members span more than one subnet.
- Uses three consecutive missed heartbeats to remove a server from the cluster membership list.

Depending on the number of servers in your cluster and on whether the cluster membership is critical for the underlying application (for example in session-replication intensive applications or clusters with intensive RMI invocations across the cluster), each model may behave better.

Consider whether your topology is going to be part of an Active-Active disaster recovery system or if the cluster is going to traverse multiple subnets. In general, unicast will behave better in those cases.

For more information see the following resources:

- "Configuring Multicast Messaging for WebLogic Server Clusters" in the *Oracle Fusion Middleware High Availability Guide*
- "One-to-Many Communication Using Unicast" in *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*.

1.2.6.5 Understanding OPSS and Requests to the Authentication and Authorization Stores

Many of the Oracle Fusion Middleware products and components require an Oracle Platform Security Services (OPSS) security store for authentication providers (an identity store), policies, credentials, keystores, and for audit data. As a result, communications must be enabled so the Application tier can send requests to and from the security providers.

When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Authentication provider. However, for an enterprise deployment, you must use a dedicated, centralized LDAP-compliant authentication provider.

For authorization (and the policy store), the location of the security store varies, depending up on the tier:

- For the application tier, the authorization store is database-based, so frequent connections from the Oracle WebLogic Server Managed Servers to the database are required for the purpose of retrieving the required OPSS data.
- For the Web tier, the authorization store is file-based, so connections to the database are not required.

For more information about OPSS security stores, see the following sections of *Oracle Fusion Middleware Application Security Guide*:

- "Authentication Basics"
- "The OPSS Policy Model"

1.2.7 About the Data Tier

In the Data tier, an Oracle RAC database runs on the two hosts (DBHOST1 and DBHOST2). The database contains the schemas required by the Oracle SOA Suite components and the Oracle Platform Security Services (OPSS) policy store.

You can define multiple services for the different products and components in an enterprise deployment to isolate and prioritize throughput and performance accordingly. In this guide, one database service is used as an example. Furthermore, you can use other high availability database solutions to protect the database:

- Oracle Data Guard; for more information, see the *Oracle Data Guard Concepts and Administration*
- Oracle RAC One Node; for more information, see "Overview of Oracle RAC One Node" in the *Oracle Real Application Clusters Administration and Deployment Guide*

These solutions above provide protection for the database beyond the information provided in this guide, which focuses on using an Oracle RAC Database, given the

scalability and availability requirements that typically apply to an enterprise deployment.

For more information about using Oracle Databases in a high availability environment, see "Database Considerations" in the *Oracle Fusion Middleware High Availability Guide*.

2

Understanding the IAM Enterprise Deployment

This chapter introduces and describes the Oracle Identity and Access Management deployment topologies on commodity hardware. These topologies represent specific reference implementations of the concepts described in Chapter 1, "Understanding a Typical Enterprise Deployment."

This chapter contains the following topics:

- Understanding the Primary and Build-Your-Own Enterprise Deployment Topologies
- Diagrams of the Primary Oracle Identity and Access Management Topology
- Understanding the Primary Oracle Identity and Access Management Topology Diagrams
- Using the Identity and Access Management Deployment Wizard
- Roadmap for Implementing the Primary IAM Suite Topologies
- Building your Own Oracle Identity and Access Management Topology
- About Using Server Migration to Enable High Availability of the Oracle Identity and Access Management Enterprise Topology

2.1 Understanding the Primary and Build-Your-Own Enterprise Deployment Topologies

This guide focuses on two primary reference topologies for Oracle Identity and Access Management. The components installed into each topology are the same. The difference being that one deployment is concentrated onto a small number of highly specified servers and the second is distributed amongst a larger number of smaller machines.

The exact Oracle Identity and Access Management topology you install and configure for your organization might vary, but for the two primary topologies, this guide provides step-by-step instructions for installing and configuring those topologies. To simplify the installation and configuration process this guide utilizes the IAM deployment wizard, which once you tell it how to layout your topology will automatically configure it for you.

Once you have created your deployment, this guide will show you how to extend it to include additional IAM products, which you may wish to use. The procedures in this book do not cover every IAM product. The steps in this guide can easily be adapted to any other IAM product you may wish to include.

2.2 Diagrams of the Primary Oracle Identity and Access Management Topology

The following sections provide diagrams of the two primary Oracle Identity and Access Management enterprise deployment topologies:

- Diagram of Oracle Identity and Access Management on Consolidated Hardware
- Diagram of Oracle Identity and Access Management on Distributed Hardware

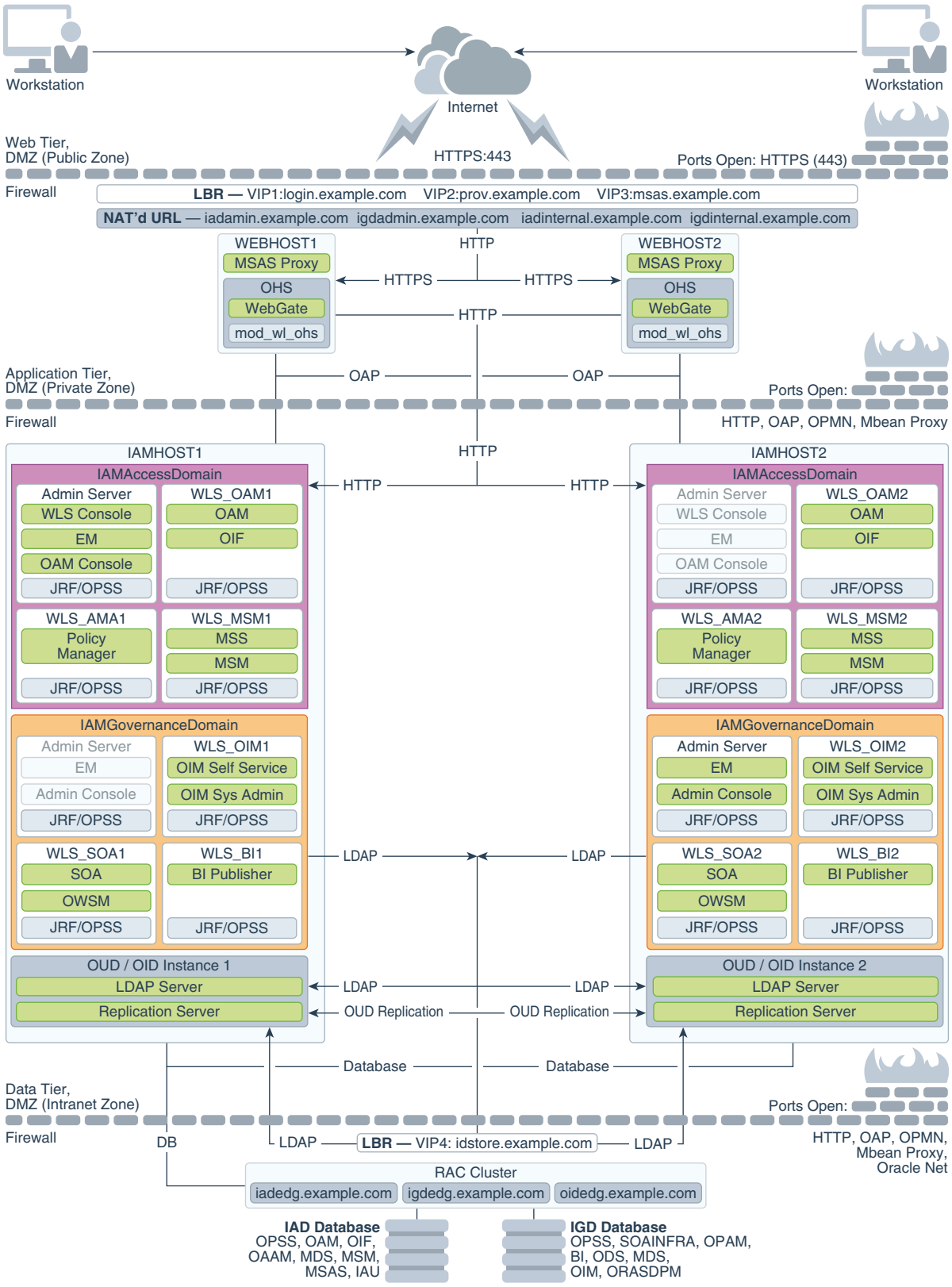
2.2.1 Diagram of Oracle Identity and Access Management on Consolidated Hardware

Figure 2–1 shows a diagram of the four-node topology with Oracle HTTP Server.

In this topology, the software is consolidated on a limited number of hosts: two hosts for the Web tier and two hosts for the application tier. You deploy both Oracle Access Management and Oracle Identity Manager on each application tier host.

This topology is a typical deployment if you are using relatively powerful, physical host computers. For information about the system requirements for each host, see Section 5.1.2, "Host Computer Hardware Requirements".

Figure 2–1 Four-Node Topology with Oracle HTTP Server


Workstation
Internet
Workstation
Web Tier,
DMZ (Public Zone)
HTTPS:443
Ports Open: HTTPS (443)
Firewall
LBR — VIP1:login.example.com VIP2:prov.example.com VIP3:msas.example.com
NAT'd URL — iadmin.example.com igdadmin.example.com iadinternal.example.com igdinternal.example.com
WEBHOST1
MSAS Proxy
OHS
WebGate
mod_wl_ohs
HTTP
HTTPS
HTTPS
WEBHOST2
MSAS Proxy
OHS
WebGate
mod_wl_ohs
HTTP
Application Tier,
DMZ (Private Zone)
OAP
OAP
Ports Open:
Firewall
HTTP, OAP, OPMN, Mbean Proxy
HTTP
IAMHOST1
IAMAccessDomain
Admin Server
WLS Console
EM
OAM Console
JRF/OPSS
WLS_OAM1
OAM
OIF
JRF/OPSS
WLS_AMA1
Policy Manager
JRF/OPSS
WLS_MSM1
MSS
MSM
JRF/OPSS
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA1
SOA
OWSM
JRF/OPSS
WLS_BI1
BI Publisher
JRF/OPSS
OUD / OID Instance 1
LDAP Server
Replication Server
HTTP
HTTP
IAMHOST2
IAMAccessDomain
Admin Server
WLS Console
EM
OAM Console
JRF/OPSS
WLS_OAM2
OAM
OIF
JRF/OPSS
WLS_AMA2
Policy Manager
JRF/OPSS
WLS_MSM2
MSS
MSM
JRF/OPSS
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA2
SOA
OWSM
JRF/OPSS
WLS_BI2
BI Publisher
JRF/OPSS
OUD / OID Instance 2
LDAP Server
Replication Server
LDAP
LDAP
LDAP
LDAP
OUD Replication
OUD Replication
Database
Database
Data Tier,
DMZ (Intranet Zone)
Ports Open:
Firewall
DB
LDAP
LBR — VIP4: idstore.example.com
LDAP
HTTP, OAP, OPMN,
Mbean Proxy,
Oracle Net
RAC Cluster
iadedg.example.com
igdedg.example.com
oidedg.example.com
IAD Database
OPSS, OAM, OIF,
OAAM, MDS, MSM,
MSAS, IAU
IGD Database
OPSS, SOAINFRA, OPAM,
BI, ODS, MDS,
OIM, ORASDPM

2.2.2 Diagram of Oracle Identity and Access Management on Distributed Hardware

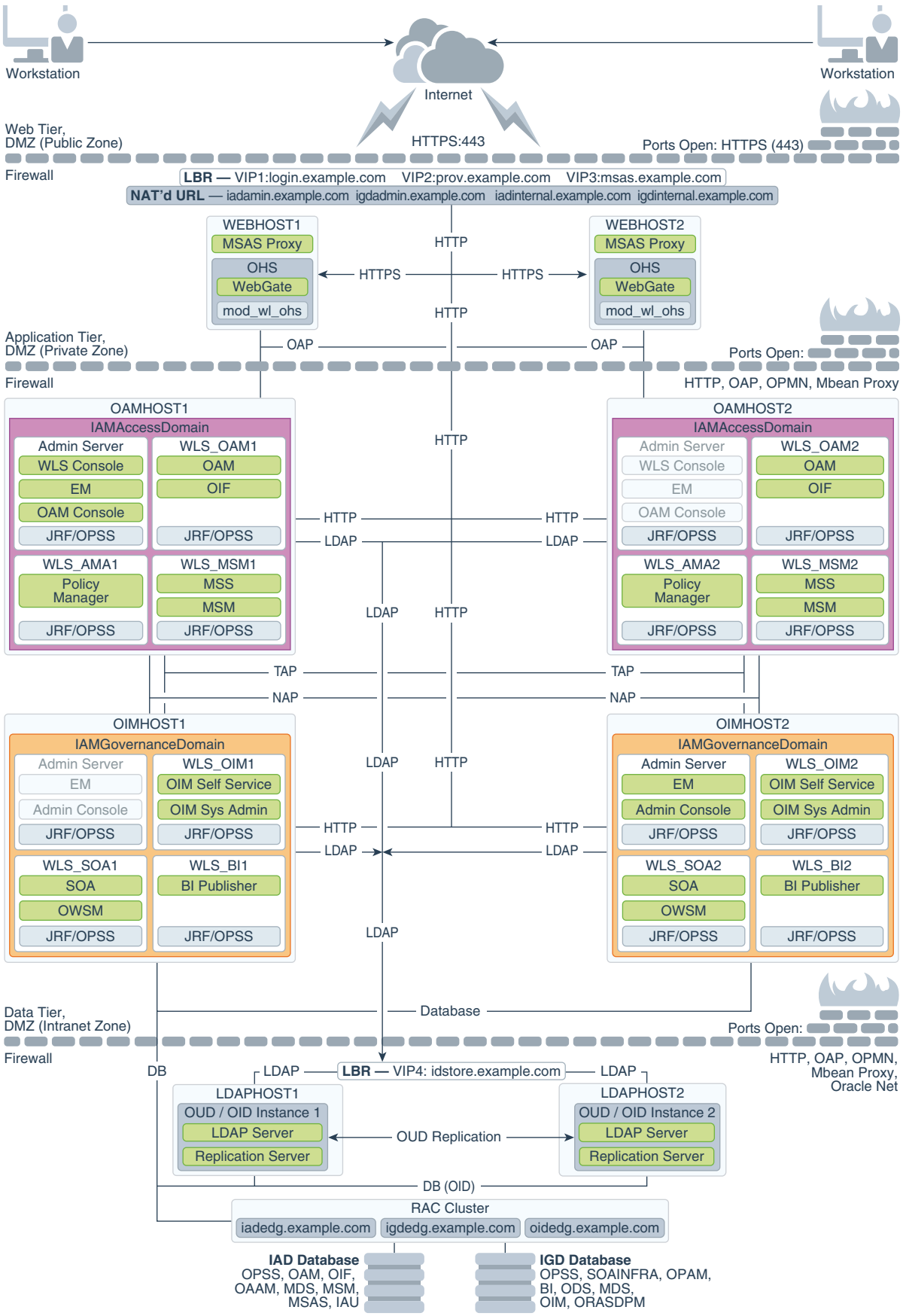
Figure 2–2 shows a diagram of the eight-node distributed topology.

In this topology, the software is distributed across eight hosts: two hosts for the Web tier and four hosts for the application tier, and four hosts for the directory services.

This topology is a typical deployment if you are using virtual machines (VMs) that are less powerful, but easy to create and manage. You deploy key components, such as Oracle Access Manager, Oracle Identity Manager, and Directory Services on their own dedicated hosts.

For information about the system requirements for each host, see Section 5.1.2, "Host Computer Hardware Requirements".

Figure 2–2 Eight-Node Distributed Topology


Workstation
Internet
Workstation
Web Tier,
DMZ (Public Zone)
HTTPS:443
Ports Open: HTTPS (443)
Firewall
LBR — VIP1:login.example.com VIP2:prov.example.com VIP3:msas.example.com
NAT'd URL — iadmin.example.com igdadmin.example.com iadinternal.example.com igdinternal.example.com
WEBHOST1
MSAS Proxy
OHS
WebGate
mod_wl_ohs
WEBHOST2
MSAS Proxy
OHS
WebGate
mod_wl_ohs
HTTP
HTTPS
HTTPS
HTTP
Application Tier,
DMZ (Private Zone)
OAP
OAP
Ports Open:
HTTP, OAP, OPMN, Mbean Proxy
Firewall
OAMHOST1
IAMAccessDomain
Admin Server
WLS Console
EM
OAM Console
JRF/OPSS
WLS_OAM1
OAM
OIF
JRF/OPSS
WLS_AMA1
Policy Manager
JRF/OPSS
WLS_MSM1
MSS
MSM
JRF/OPSS
OAMHOST2
IAMAccessDomain
Admin Server
WLS Console
EM
OAM Console
JRF/OPSS
WLS_OAM2
OAM
OIF
JRF/OPSS
WLS_AMA2
Policy Manager
JRF/OPSS
WLS_MSM2
MSS
MSM
JRF/OPSS
HTTP
HTTP
LDAP
LDAP
HTTP
HTTP
LDAP
TAP
TAP
NAP
NAP
OIMHOST1
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA1
SOA
OWSM
JRF/OPSS
WLS_BI1
BI Publisher
JRF/OPSS
OIMHOST2
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA2
SOA
OWSM
JRF/OPSS
WLS_BI2
BI Publisher
JRF/OPSS
LDAP
HTTP
HTTP
HTTP
LDAP
LDAP
LDAP
Data Tier,
DMZ (Intranet Zone)
Database
Ports Open:
HTTP, OAP, OPMN,
Mbean Proxy,
Oracle Net
Firewall
DB
LDAP
LBR — VIP4: idstore.example.com
LDAP
LDAPHOST1
OUD / OID Instance 1
LDAP Server
Replication Server
OUD Replication
LDAPHOST2
OUD / OID Instance 2
LDAP Server
Replication Server
DB (OID)
RAC Cluster
iadedg.example.com
igdedg.example.com
oidedg.example.com
IAD Database
OPSS, OAM, OIF,
OAAM, MDS, MSM,
MSAS, IAU
IGD Database
OPSS, SOAINFRA, OPAM,
BI, ODS, MDS,
OIM, ORASDPM

2.3 Understanding the Primary Oracle Identity and Access Management Topology Diagrams

This section describes the Primary Oracle Identity and Access Management Topology diagrams.

This section contains the following topics:

2.3.1 Product Separation

An IAM deployment is made up of a number of components. These components include:

- Web Servers
- WebLogic
- LDAP
- Database

Figure 2–1 and Figure 2–2 depict a separation between each component. The Oracle Identity and Access Management components are split into two different domains: IAMAccessDomain and IAMGovernanceDomain. Products are distributed as follows:

- IAMAccessDomain contains Oracle Access Manager, Oracle Mobile Security Suite, Oracle Adaptive Access Manager.
- IAMGovernanceDomain contains Oracle Identity Manager, Oracle Business Intelligence, Oracle Privileged Account Manger.

This split is due to the different operational and availability requirements demanded of the individual components. Typically components in the IAMAccessDomain have a higher availability requirement than those in the IAMGovernanceDomain. By separating these components out, you can manage the availability requirements differently. You can patch governance components independently of access components, and you can shutdown the governance instance without impacting the access components.

This separation is extended to the Directory tier as well, which is often released at a different time to that of the Web tier and the Application tier components. Separation of the directory provides the same benefits as splitting the domains, for example, Independent upgrade and patching.

A further benefit of this separation is that you can build a topology in a modular fashion. You can start off with a directory and extend it to Access Components, then later extend it to Governance components, without needing to affect the deployed software or configuration of existing components, unless you are wiring them together.

2.3.2 Understanding the Directory Tier

The Directory tier consists of two physical host computers, where an LDAP compliant directory is installed. Typically, this is Oracle Internet Directory (OID) or Oracle Unified Directory (OUD).

The Directory tier is often combined with the Data tier.

This release of the Enterprise Deployment Guide supports three different LDAP directories. You may be creating these directories for the first time, or you may be using existing directories from within the organization. The different directories supported are:

- Oracle Unified Directory (OUD)
- Oracle Internet Directory (OID)
- Microsoft Active Directory (AD)

The directory you choose will be organization dependent.

2.3.3 Understanding Oracle Unified Directory Assured Replication

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

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

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

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

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

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

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

2.3.4 Summary of Oracle Identity and Access Management Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, a hardware load balancer is required. This hardware load balancer should exist on redundant hardware to ensure maximum availability. The hardware load balancer must be configured to recognize a set of virtual server names.

The hardware load balancer in Oracle Identity and Access Management deployments must recognize the following virtual server names.

- `login.example.com` - This virtual server name is used for all incoming Access traffic. It acts as the access point for all HTTP traffic to the runtime Access Management components. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  `login.example.com:443`

- `prov.example.com` - This virtual server name is used for all incoming Governance traffic. It acts as the access point for all HTTP traffic to the runtime Governance components. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  `prov.example.com:443`

  Note that, in previous releases of the Enterprise Deployment Guide, `login.example.com` and `prov.example.com` were the same entry point. This release allows for them to be separated out. This will enable smarter routing from the load balancer, allow a more modular deployment and will facilitate future Multi-datacenter deployments. If desired these two entry points can still be combined to provide a single point of entry into the IAM deployment.

- `msas.example.com` - This virtual server name is used for all incoming Mobile Security traffic. It acts as the access point for all HTTPS traffic to the runtime Mobile Security Access Service. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  `msas.example.com:9002`

- `iadadmin.example.com` - This virtual server name is enabled on the load balancer. It acts as the access point for all internal HTTP traffic that gets directed to the administration services in the IAMAccessDomain. The incoming traffic from clients is non-SSL enabled. Therefore, the clients access this service using the following address:

  `iadadmin.example.com:80`

  This in turn is forwarded to port `7777` on WEBHOST1 and WEBHOST2.

  The services accessed on this virtual host include the WebLogic Administration Server Console and Oracle Enterprise Manager Fusion Middleware Control.

  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 iadadmin.example.com virtual host.

- `igdadmin.example.com` - This virtual server name is enabled on the load balancer. It acts as the access point for all internal HTTP traffic that gets directed to the administration services in the IAMGovernanceDomain. The incoming traffic from

clients is non-SSL enabled. Therefore, the clients access this service using the following address:

igdadmin.example.com:80

This in turn is forwarded to port 7777 on WEBHOST1 and WEBHOST2.

The services accessed on this virtual host include the WebLogic Administration Server Console and Oracle Enterprise Manager Fusion Middleware Control.

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 igdadmin.example.com virtual host.

- iadinternal.example.com - This virtual server name is for internal communications between the application tier components in the Access Domain only and is not exposed to the Internet. The primary use of this virtual server is to allow the Mobile Security Access Service to communicate with either the Oracle HTTP server, which is being used to distribute requests to Oracle Mobile Security Manager, or it can be used to send requests directly to the WebLogic Managed Servers hosting Mobile Security Manager.

  The traffic from clients to this virtual server is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  iadinternal.example.com:7777

- igdinternal.example.com - This virtual server name is for internal communications between the application tier components in the Governance Domain only and is not exposed to the Internet. This virtual server is used for both Oracle OIM Suite and Oracle SOA Suite internal communications.

  The traffic from clients to this virtual server is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  igdinternal.example.com:80

- idstore.example.com - This virtual server name is used for all incoming identity store traffic. It acts as the access point to the LDAP directory instances. This virtual server is not exposed to the internet.

  The traffic from clients to this virtual server may or may not be SSL-enabled, depending on the type of LDAP directory in use. Typically, this will be non-SSL enabled for Oracle Unified Directory and Oracle Internet Directory and enabled for Microsoft Active Directory. Clients access this service using this virtual server name and the requests are forwarded to the LDAP instances.

2.3.5 Summary of the Managed Servers and Clusters on the Application Tier Hosts

The Application tier hosts the Administration Server and Managed Servers in the Oracle WebLogic Server domains.

Depending upon the components you select, the Oracle WebLogic Server domain for the Oracle Identity and Access Management consists of the clusters shown in Table 2–1. These clusters function as active-active high availability configurations.

Table 2–1 Domain Clusters and Managed Servers

Domain	Cluster	Managed Servers
IAMAccessDomain	Oracle Access Manager	wls_oam1, wls_oam2

Table 2–1 (Cont.) Domain Clusters and Managed Servers

Domain	Cluster	Managed Servers
	Oracle Policy Manager	wls_ama1, wls_ama2
	Oracle Mobile Security Manager	wls_msm1, wls_msm2
IAMGovernanceDomain	Oracle Identity Manager	wls_oim1, wls_oim2
	Oracle SOA Suite	wls_soa1, wls_soa2
	Oracle Business Intelligence	wls_bi1, wls_bi2

2.3.6 Understanding Mobile Security Access Server

The Mobile Security Access Server is used to serve requests from Mobile Security clients.

Mobile clients access the load balancer using the HTTPS protocol. The load balancer then forwards those requests to the Mobile Security Access server using HTTPS. The Mobile Security Server then interacts with the Oracle Mobile Security Managed Servers through the Oracle HTTP Server. These requests are sent using HTTP.

Figure 1–1, "Typical Enterprise Deployment Topology Diagram" shows these requests going through the main Oracle HTTP servers. It is possible to increase performance by directing the request to dedicated Oracle HTTP Servers (which do not have Web gate configured), or alternatively, to the Mobile Security managed servers directly through another load balancer.

- MSAS can continue to operate while MSM is down. This is known as the disconnected mode of operation. In this mode – MSAS will not pull any management/artifact changes done via the UI or WLST in MSM – but will continue to enforce security.

  Note: MSAS needs MSM to be up and running when `configMSAS` is run to create an instance. Therefore, MSAS must connect at least once to MSM.

- MSAS has a persistent local file-based cache. So MSAS can be taken down and brought back up and should continue to operate.
- There are number of message exchanges through Secure Mobile Container and MSAS during authentication (KINIT/PKINIT/OAuth). The end result of the authentication process is the creation of a Session Token (STOKEN). The load balancer session must be sticky during the authentication process (usually 1 SSL connection), but not for subsequent requests.

  MSAS has dedicated authentication urls and so we will need to configure the MSAS authentication urls to be sticky.

  Note: If the load balancer is not sticky during the authentication process – there is no guarantee that authentication will succeed.

- There is a session synchronization through MSAS physical instances. So if the STOKEN (Session Token) is created by MSAS instance running on Host 1 initially,

and subsequent load balancing results in the mobile traffic being routed to Host 2, the MSAS instance running on Host 2 automatically connects to Host 1 for the STOKEN.

> **Note:** Since Host 2 needs to connect to Host#1 at-least once (if the original STOKEN was created by Host 1), Host 1 must be up and running at that time. However once Host 2 has connected with Host 1, Host 1 can fail.

In ability to perform session sync results in having to log in again. The session synchronization using multiple MSAS physical instances happens over HTTP(S).

- Some of the authentication scenarios require one-way SSL, or two-way SSL using the Mobile Secure Container and MSAS. As long as the MSAS physical instances are configured with the same MSAS Instance ID (a single logical instance), MSAS ensures the SSL certificates and keys, are replicated automatically to all the physical instances.
- MSAS supports automatic recovery from failures at the MSAS physical instance level. When you create and run an MSAS instance (physical), it starts a heartbeat process that is created and runs in the background. This heartbeat process is local to the instance and monitors/pings the MSAS instance to check if it is alive. If not, it tries to restart the MSAS instance. The number of attempts to restart the MSAS instance, is configurable. The heartbeat process uses UDP to ping MSAS.

2.4 Using the Identity and Access Management Deployment Wizard

This guide makes use of the new Identity and Access Management Deployment Tool. It is also possible to create the deployment manually. The benefits of using the deployment tool are:

- Simplified wizard driven deployment.
- EDG Best practices incorporated into the tool.
- Faster more reliable deployment of the Enterprise Deployment topology.
- Access to post deployment life cycle management tools such as simpler patch application.

The deployment tool does not build all deployments but it speeds up the building of those parts of the deployment it does address. Extending the deployment beyond the products included in the deployment tool is still a manual task, which is covered by this guide.

2.5 Roadmap for Implementing the Primary IAM Suite Topologies

Table 2–2 provides a roadmap for implementing the primary IAM suite topologies on commodity hardware.

Table 2–2 Roadmap for Implementing Primary IAM Suite Topologies on Commodity Hardware

Scenario	Tasks	For More Information, See
Creating an IAM Enterprise Deployment manually on commodity hardware	Understand a typical enterprise deployment and review the primary deployment topologies.	Chapter 1, "Understanding a Typical Enterprise Deployment" Section 2.2, "Diagrams of the Primary Oracle Identity and Access Management Topology" Section 2.3, "Understanding the Primary Oracle Identity and Access Management Topology Diagrams"
	Review the hardware and software requirements and procure the resources for the enterprise deployment.	Chapter 5, "Procuring Resources for an Enterprise Deployment"
	Prepare the load balancers and firewalls.	Chapter 6, "Preparing the Load Balancer and Firewalls for an Enterprise Deployment"
	Prepare the storage and understand the directory structure.	Chapter 7, "Preparing Storage for an Enterprise Deployment"
	Configure the host computers.	Chapter 9, "Configuring the Host Computers for an Enterprise Deployment"
	Prepare the database.	Chapter 10, "Preparing the Database for an Enterprise Deployment"
	Install the required softwares.	Chapter 11, "Installing Oracle Fusion Middleware in Preparation for an Enterprise Deployment"
	Configure Oracle LDAP.	Chapter 12, "Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment"
	Prepare the identity store.	Chapter 13, "Preparing The Identity Store"
	Configure the Oracle Web Tier.	Chapter 14, "Configuring the Oracle Web Tier"
	Create the WebLogic domains.	Chapter 15, "Creating Domains for an Enterprise Deployment"
	Set up the Node Manager.	Chapter 16, "Setting Up Node Manager for an Enterprise Deployment"
	Configure Oracle Access Management (OAM).	Chapter 17, "Configuring Oracle Access Management"
	Configure Oracle Mobile Security Services (OMSS).	Chapter 18, "Configuring Oracle Mobile Security Services"
	Configure Oracle Identity Manager (OIM).	Chapter 19, "Configuring Oracle Identity Manager"
	Configure Oracle BI Publisher (BIP).	Chapter 20, "Configuring BI Publisher"

Table 2–2 (Cont.) Roadmap for Implementing Primary IAM Suite Topologies on Commodity Hardware

Scenario	Tasks	For More Information, See
Creating an IAM Enterprise Deployment using Life Cycle Management Tools (IDMLCM), on commodity hardware	Understand the automated deployment process.	Chapter 23, "Introduction to the Life Cycle Management (LCM) Tools"
	Install the Oracle Identity and Access Management Life Cycle Management Tools.	Chapter 24, "Installing Oracle Identity and Access Management Life Cycle Management Tools"
	Create a deployment response file for the topology you are deploying.	Chapter 25, "Creating a Deployment Response File"
	Deploy Identity and Access Management.	Chapter 26, "Deploying Identity and Access Management"
	Perform the required post-deployment tasks.	Chapter 27, "Performing Post-Deployment Configuration"

2.6 Building your Own Oracle Identity and Access Management Topology

This document provides step-by-step instructions for configuring the two primary enterprise topologies for Oracle Identity and Access Management.

However, Oracle recognizes that the requirements of your organization may vary, depending on the specific set of Oracle Fusion Middleware products you purchase and the specific types of applications you deploy.

In many cases, you can install and configure an alternative topology--one that includes additional components, or one that does not include all the Oracle SOA Suite products shown in the primary topology diagrams.

The following sections describe some alternative Oracle Identity and Access Management topologies you can implement, using some variations of the instructions in this guide. For more information, refer to the resources available on the Oracle Maximum Availability Architecture (MAA) Web site.

- OAM Only with an Existing Directory
- OAM Only with OAAM
- OIM Only with an Existing Directory
- OIM Only with OPAM
- OAM/OIM Integrated in a Modular Deployment
- OAM/OIM Integrated with an Existing Directory
- OAM/OIM with OAAM
- OAM/OIM with OPAM

2.7 About Using Server Migration to Enable High Availability of the Oracle Identity and Access Management Enterprise Topology

To ensure high availability of the Oracle Identity and Access Management Suite products and components, this guide recommends that you enable Oracle WebLogic Server Whole Server Migration for the Oracle Identity Manager, Oracle SOA Suite, and Oracle Business Intelligence clusters that you create as part of the reference topology.

Whole server migration provides for the automatic restart of a server instance, with all of its services, on a different physical machine. When a failure occurs in a server that is part of a cluster that is configured with server migration, the server is restarted on any of the other machines that host members of the cluster.

For more information, see Chapter 21, "Configuring Server Migration for an Enterprise Deployment."

3

Understanding the IAM Exalogic Enterprise Deployment

This chapter introduces and describes the Oracle Identity and Access Management deployment topologies on Exalogic hardware. These topologies represent specific reference implementations of the concepts described in Chapter 1, "Understanding a Typical Enterprise Deployment."

- Why Install Oracle IAM on Exalogic
- Understanding the Primary and Build your Own Enterprise Deployment Topologies on Exalogic
- Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies
- Oracle Identity and Access Management and Exalogic Networking
- Summary of the Managed Servers and Clusters on the Application Tier Hosts
- Understanding Oracle Traffic Director
- About Exalogic Optimizations for WebLogic
- Roadmap for Implementing the Primary Oracle Identity and Access Management Topologies
- Building your Own Oracle Identity and Access Management Topology
- About Installing and Configuring a Custom Enterprise Topology
- About Using Server Migration to Enable High Availability of the Oracle Identity and Access Management Enterprise Topology

This book assumes you have an understanding of Exalogic, if you wish to gain further information on how Exalogic works, refer to the *Enterprise Deployment Guide for Exalogic* for the release of Exalogic you are using.

3.1 Why Install Oracle IAM on Exalogic

Oracle Exalogic is a highly available, high performance integrated hardware appliance from Oracle. Oracle Fusion Middleware components, when deployed onto Oracle Exalogic, get the benefit of its superior networking, resulting in improved application throughput. In addition, WebLogic server has had a number of optimizations that enable it to run faster on Oracle Exalogic. These optimizations further increase the throughput of the applications deployed.

Deploying Oracle IAM on Exalogic ensures that you have a highly available infrastructure that provides you with the maximum availability and performance available.

3.2 Understanding the Primary and Build your Own Enterprise Deployment Topologies on Exalogic

This guide focuses on three primary reference topologies for Oracle Identity and Access Management (IAM) Suite on Exalogic. The components installed into each topology are essentially the same. These topologies are very similar to the platform topologies in that they are distributed topologies which are more suited to virtual Exalogic deployments, and a consolidated topology which is more suited to Physical Exalogic deployments. There is, however, a third topology which is a hybrid topology that uses some components installed in Exalogic and others, for example, the Web tier, installed on commodity hardware outside of the Exalogic machine.

The exact Oracle Identity and Access Management topology you install and configure for your organization might vary, but for the three primary topologies, this guide provides step-by-step instructions for installation and configuration of the topologies. To simplify the installation and configuration process, this guide utilizes the Oracle IAM deployment Wizard, which, once you set it up to layout your topology, will automatically configure the majority of it for you.

Once you have created your deployment, this guide provides instructions for extending the deployment to include additional IAM products. In addition, while procedures in this book do not cover every IAM product, these steps can easily be adapted to any other IAM product.

3.3 Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies

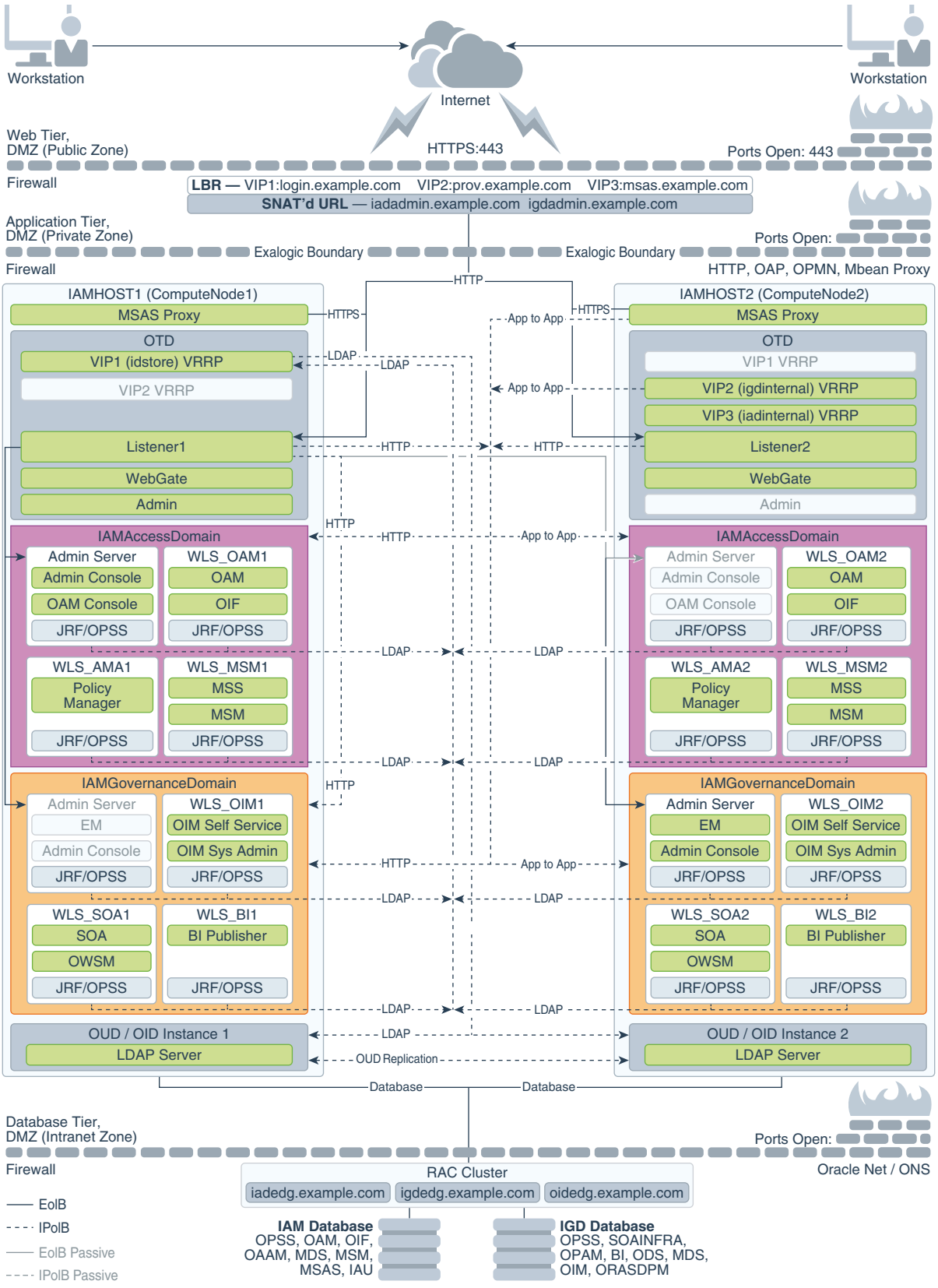
This diagrams in this section illustrate Oracle IAM Exalogic topologies.

This section contains the following topics:

3.3.1 Diagram of Oracle Identity and Access Management on Physical Exalogic

Figure 3–1 illustrates the Oracle Identity and Access Management consolidated topology.

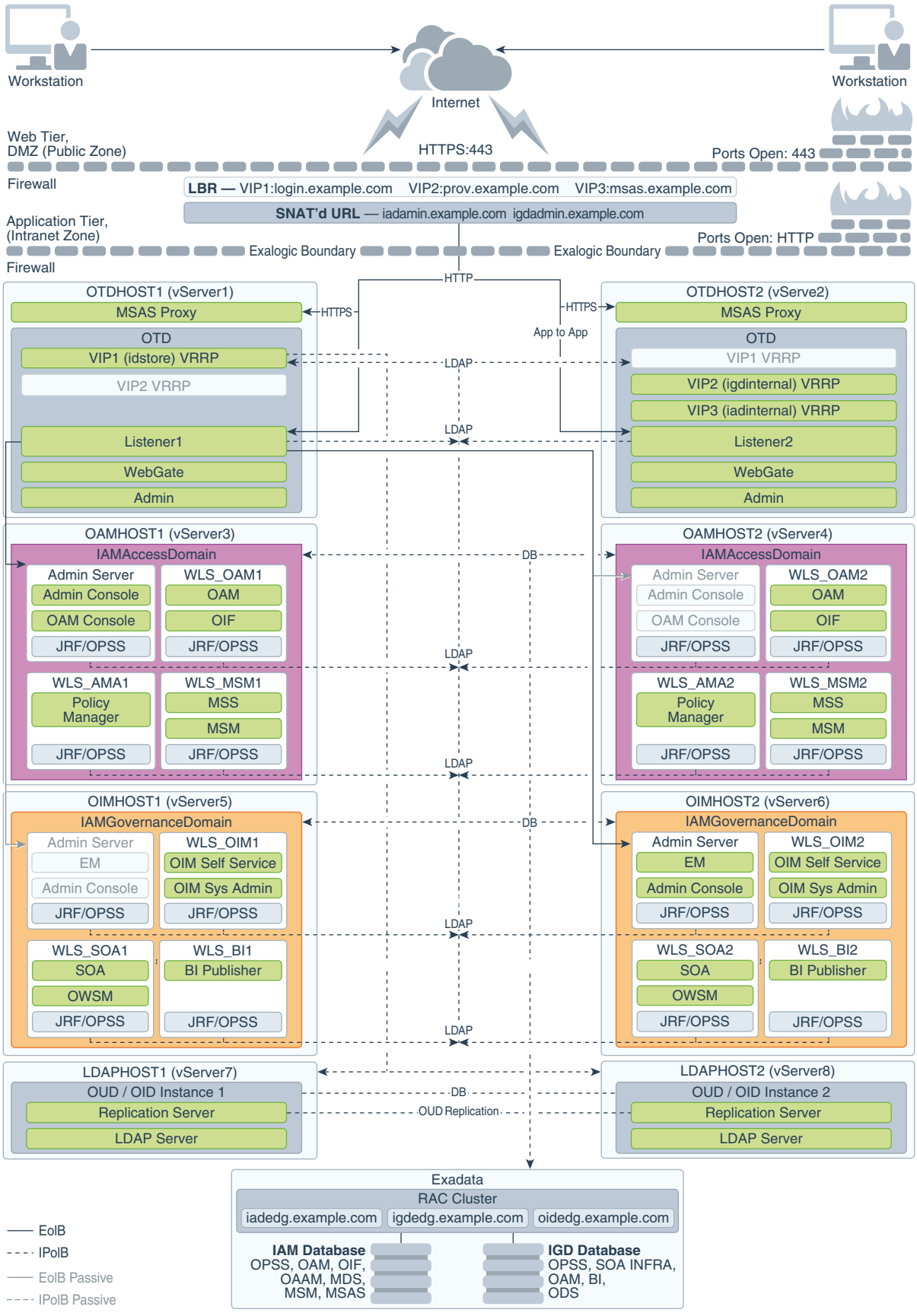
Figure 3–1 Exalogic Physical Deployment Topology



3.3.2 Diagram of Oracle Identity and Access Management on Virtual Exalogic

Figure 3–2 illustrates the Oracle Identity and Access Management distributed topology.

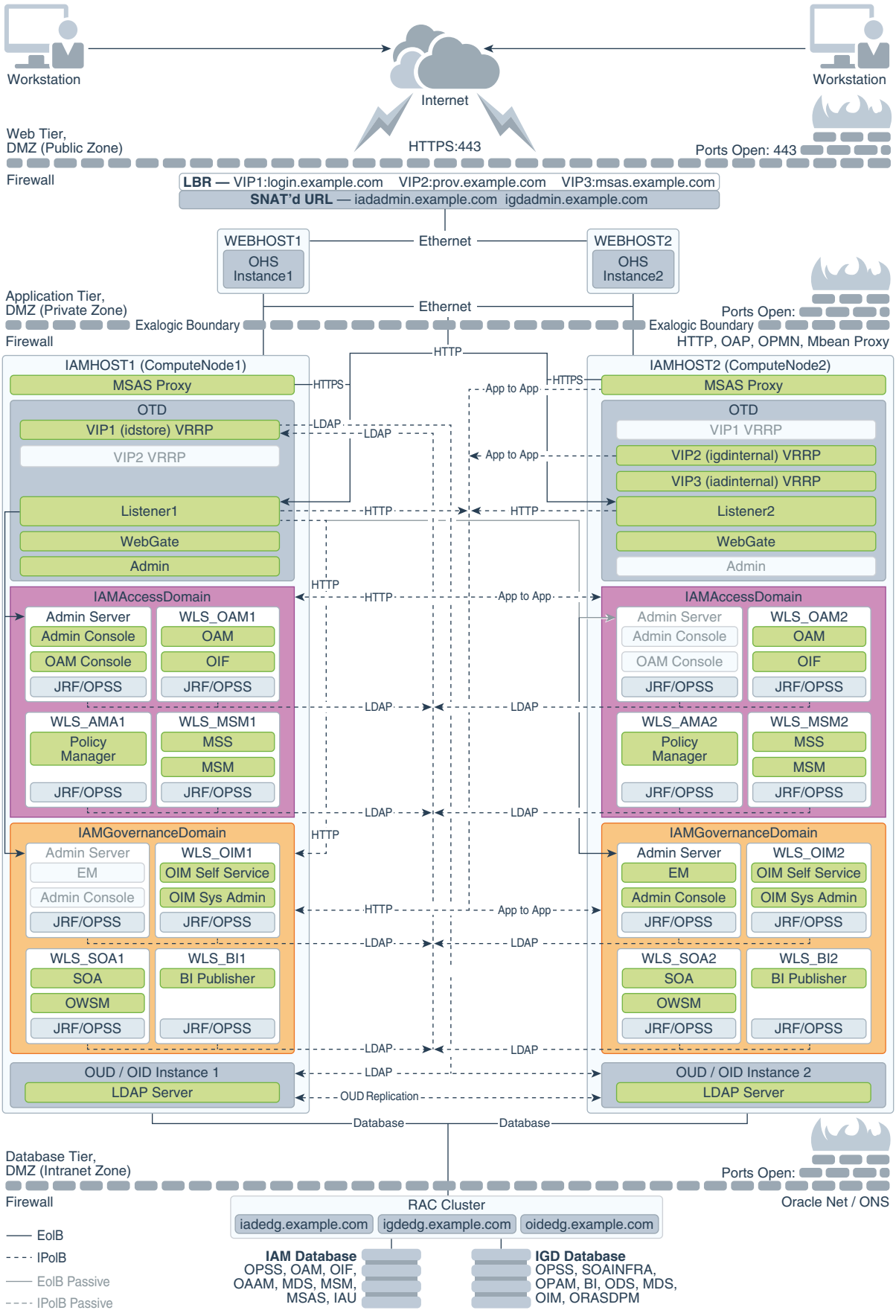
Figure 3–2 Exalogic Virtual Deployment Topology Diagram


Workstation
Internet
Workstation
Web Tier,
DMZ (Public Zone)
HTTPS:443
Ports Open: 443
Firewall
LBR — VIP1:login.example.com VIP2:prov.example.com VIP3:msas.example.com
SNAT'd URL — iadmin.example.com igdadmin.example.com
Application Tier,
(Intranet Zone)
Exalogic Boundary
Exalogic Boundary
Ports Open: HTTP
Firewall
HTTP
OTDHOST1 (vServer1)
MSAS Proxy
HTTPS
OTD
VIP1 (idstore) VRRP
VIP2 VRRP
Listener1
WebGate
Admin
HTTPS
App to App
OTDHOST2 (vServe2)
MSAS Proxy
OTD
VIP1 VRRP
VIP2 (igdinternal) VRRP
VIP3 (iadinternal) VRRP
Listener2
WebGate
Admin
LDAP
LDAP
OAMHOST1 (vServer3)
IAMAccessDomain
Admin Server
Admin Console
OAM Console
JRF/OPSS
WLS_OAM1
OAM
OIF
JRF/OPSS
WLS_AMA1
Policy Manager
JRF/OPSS
WLS_MSM1
MSS
MSM
JRF/OPSS
DB
OAMHOST2 (vServer4)
IAMAccessDomain
Admin Server
Admin Console
OAM Console
JRF/OPSS
WLS_OAM2
OAM
OIF
JRF/OPSS
WLS_AMA2
Policy Manager
JRF/OPSS
WLS_MSM2
MSS
MSM
JRF/OPSS
LDAP
LDAP
OIMHOST1 (vServer5)
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA1
SOA
OWSM
JRF/OPSS
WLS_BI1
BI Publisher
JRF/OPSS
DB
OIMHOST2 (vServer6)
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Self Service
OIM Sys Admin
JRF/OPSS
WLS_SOA2
SOA
OWSM
JRF/OPSS
WLS_BI2
BI Publisher
JRF/OPSS
LDAP
LDAP
LDAPHOST1 (vServer7)
OUD / OID Instance 1
Replication Server
LDAP Server
DB
OUD Replication
LDAPHOST2 (vServer8)
OUD / OID Instance 2
Replication Server
LDAP Server
Exadata
RAC Cluster
iadedg.example.com
igdedg.example.com
oidedg.example.com
IAM Database
OPSS, OAM, OIF,
OAAM, MDS,
MSM, MSAS
IGD Database
OPSS, SOA INFRA,
OAM, BI,
ODS
EoIB
IPoIB
EoIB Passive
IPoIB Passive

3.3.3 Diagram of Oracle Identity and Access Management with an External Web Tier

Figure 3–3illustrates the Oracle Identity and Access Management consolidated topology with an external Web tier.

Figure 3–3 Exalogic Topology with External OHS


Workstation
Internet
Workstation
Web Tier,
DMZ (Public Zone)
HTTPS:443
Ports Open: 443
Firewall
LBR — VIP1:login.example.com VIP2:prov.example.com VIP3:msas.example.com
SNAT'd URL — iadadmin.example.com igdadmin.example.com
WEBHOST1
OHS Instance1
Ethernet
WEBHOST2
OHS Instance2
Application Tier,
DMZ (Private Zone)
Ethernet
Ports Open:
Exalogic Boundary
Exalogic Boundary
Firewall
HTTP, OAP, OPMN, Mbean Proxy
HTTP
IAMHOST1 (ComputeNode1)
IAMHOST2 (ComputeNode2)
MSAS Proxy
HTTPS
App to App
HTTPS
MSAS Proxy
OTD
VIP1 (idstore) VRRP
LDAP
LDAP
VIP2 VRRP
OTD
VIP1 VRRP
App to App
VIP2 (igdinternal) VRRP
VIP3 (iadinternal) VRRP
Listener1
HTTP
HTTP
Listener2
WebGate
Admin
WebGate
Admin
HTTP
IAMAccessDomain
HTTP
App to App
IAMAccessDomain
Admin Server
Admin Console
OAM Console
JRF/OPSS
WLS_OAM1
OAM
OIF
JRF/OPSS
Admin Server
Admin Console
OAM Console
JRF/OPSS
WLS_OAM2
OAM
OIF
JRF/OPSS
LDAP
LDAP
WLS_AMA1
Policy Manager
JRF/OPSS
WLS_MSM1
MSS
MSM
JRF/OPSS
WLS_AMA2
Policy Manager
JRF/OPSS
WLS_MSM2
MSS
MSM
JRF/OPSS
LDAP
LDAP
IAMGovernanceDomain
HTTP
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Self Service
OIM Sys Admin
JRF/OPSS
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Self Service
OIM Sys Admin
JRF/OPSS
HTTP
App to App
LDAP
LDAP
WLS_SOA1
SOA
OWSM
JRF/OPSS
WLS_BI1
BI Publisher
JRF/OPSS
WLS_SOA2
SOA
OWSM
JRF/OPSS
WLS_BI2
BI Publisher
JRF/OPSS
LDAP
LDAP
OUD / OID Instance 1
LDAP Server
LDAP
OUD Replication
OUD / OID Instance 2
LDAP Server
Database
Database
Database Tier,
DMZ (Intranet Zone)
Ports Open:
Firewall
Oracle Net / ONS
RAC Cluster
iadedg.example.com
igdedg.example.com
oidedg.example.com
EoIB
IPoIB
EoIB Passive
IPoIB Passive
IAM Database
OPSS, OAM, OIF,
OAAM, MDS, MSM,
MSAS, IAU
IGD Database
OPSS, SOAINFRA,
OPAM, BI, ODS, MDS,
OIM, ORASDPM

3.3.4 Understanding the Primary Oracle Identity and Access Management Topology Diagrams

This section describes the Primary Oracle Identity and Access Management Topology diagrams.

This section contains the following topics:

3.3.4.1 About Product Separation

An Oracle Identity and Access Management deployment is made up of a number of components. These components include:

- Web Servers
- WebLogic
- LDAP - Manage a Virtual IP Address that internal servers can access for the purposes of making LDAP calls.

  Receive requests on the LDAP Virtual IP address and pass them on to the running LDAP instances using the IPoIB Network.
- Database

About Access and Governance Domains

Figure 3–1, Figure 3–2, and Figure 3–3 depict a separation between each component. In addition, the WebLogic components are further split into two different WebLogic domains: IAMAccessDomain, and IAMGovernanceDomain. Products are distributed as follows:

- IAMAccessDomain contains Oracle Access Manager, Oracle Mobile Security Suite.
- IAMGovernanceDomain contains Oracle Identity Manager, Oracle Business Intelligence.

This split is due to the different operational and availability requirements demanded of the individual components. Typically components in the IAMAccessDomain have a higher availability requirement than those in the IAMGovernanceDomain. By separating these components, you can manage the availability requirements differently. You can patch governance components independently of access components, and you can shutdown the governance instance without impacting the access components.

This separation is extended to the Directory tier as well, which is often released at a different time to that of the Web tier and the Application tier components. Separation of the directory provides the same benefits as splitting the domains, for example, Independent upgrade and patching.

A further benefit of this separation is that you can build a topology in a modular fashion. You can start with a directory and extend it to Access Components, and later extend it to Governance components, without needing to affect the deployed software or configuration of existing components, unless you are wiring them together.

3.3.4.2 Understanding the Directory Tier

The Directory tier consists of two physical host computers, where an LDAP compliant directory is installed. Typically, this is Oracle Internet Directory (OID) or Oracle Unified Directory (OUD).

The Directory tier is often combined with the Data tier.

This release of the Enterprise Deployment Guide supports three different LDAP directories. You may be creating these directories for the first time, or you may be using existing directories from within the organization. The three different directories supported are:

- Oracle Unified Directory (OUD)
- Oracle Internet Directory (OID)
- Microsoft Active Directory (AD)

The directory you choose will be organization dependent.

3.3.5 Differences Between an Exalogic Deployment and a Platform Deployment

When you deploy Oracle Identity and Access Management on Exalogic, most, if not all of the components are installed inside the Exalogic appliance. As described in Chapter 1, "Understanding a Typical Enterprise Deployment," a typical enterprise deployment is distributed amongst various tiers. Because the hardware components are incorporated into the Exalogic Appliance, the number of tiers available is reduced.

There is no need for an application or directory tier and if your Exalogic Appliance is linked to an Exadata appliance. Database tier is moved to Exadata if Exalogic is linked to it.

The second major difference between a platform and an Exalogic deployment is that the Exalogic deployment use Oracle Traffic Director instead of Oracle HTTP server. In an Exalogic deployment, Oracle Traffic Director performs a number of roles. It can act as both a load balancer for internal traffic ensuring that it is not exposed outside the Exalogic Appliance, and as a Web Server.

If you use an external Web tier, you do not need to use the Web serving characteristics of Oracle Traffic Director.

When you deploy Oracle Fusion Middleware on Oracle Exalogic, you gain access to a number of in-built WebLogic optimizations which ensure that the Fusion Middleware deployment uses some of the in-built Exalogic technologies to provide better performance.

3.4 Oracle Identity and Access Management and Exalogic Networking

One of the core advantages of Exalogic is its fast and flexible network. When deploying Oracle IAM on Exalogic, you have to consider how you wish to use the Oracle Exalogic Networking.

There are three types of networks within an Exalogic appliance:

- **IPoIB** - This is the internal Infiniband Network that connects the internal components of the Exalogic appliance. This network is fast, but cannot be connected to the outside world. The benefit of this network is that it can be used to ensure that network traffic is kept private from the outside world. The downside to using this network is where external components need to access application components inside the Exalogic Appliance.

- **EoIB** - This network also uses the Exalogic Infiniband Network but it is possible to connect this network to the standard corporate network. This allows external component to communicate directly to components inside Exalogic. This network is always used for communication between your hardware load balancer and Oracle Traffic Director.
- **eth0** - This is the management network it is used for connecting to the Exalogic components through the built-in ethernet network. This network is only used for management operations and should not be used for production deployments. Its this network that is used to log in to the Exalogic components to configure them.

3.4.1 Considerations for Choosing your Exalogic Network

Some components within IAM, by default, only talk on a single network. For example, WebLogic Managed servers, other components such as Oracle Traffic Director communicate on both the internal networks. This is why Oracle Traffic Director is the preferred load balancer for traffic once it enters the Exalogic Appliance.

When choosing which Exalogic Network to use, consider the following:

- Are you planning to use an external Web tier? If so, by default, you can configure your components to work on the EoIB Network.
- If all Traffic comes through Oracle Traffic Director, and once it reaches there, all traffic stays within the Exalogic appliance, configure components to use the IPoIB network.
- If all LDAP traffic originates within the Exalogic Appliance, configure your LDAP server to use the IPoIB network.
- If your database resides in an Exadata appliance, which is directly connected to the Exalogic appliance, use the IPoIB network. If not, then you should use the EoIB network.

Note: You can configure Oracle Access Manager Managed Servers to communicate on both networks using the OAM Proxy port.

You can configure Standard WebLogic Managed Servers to listen on multiple networks using different channels.

3.4.2 Typical IAM Network Usage

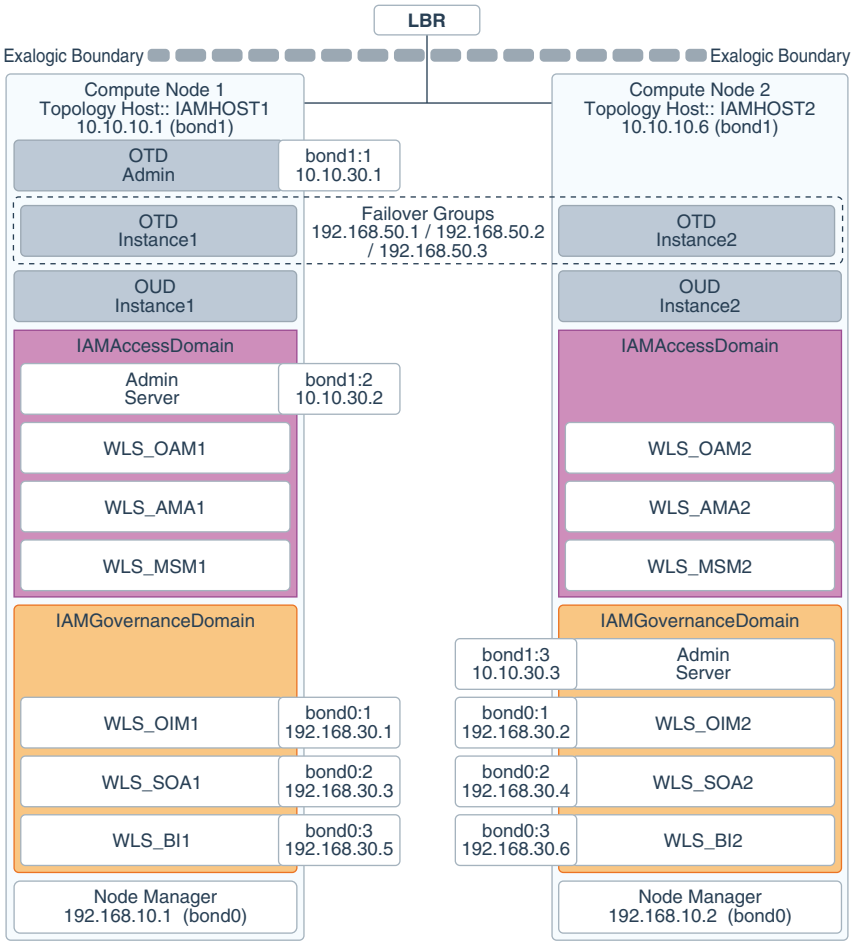
This section describes a typical IAM network usage. It contains the following sections:

- Section 3.4.2.1, "Physical Exalogic"
- Section 3.4.2.2, "Virtual Exalogic"
- Section 3.4.2.3, "Physical Exalogic with External Web Tier"

3.4.2.1 Physical Exalogic

Figure 3–4 shows the typical network map for an Identity and Access Management deployment on a physical Exalogic environment.

Figure 3–4 Physical Exalogic Network Map



The diagram is explained in the table following the image.

****

If you are not using an external Web tier, you can configure all components to use the Internal IPoIB network. Oracle traffic Director and MSAS are configured to accept requests on the EoIB network, but pass them on to WebLogic and LDAP using the IPoIB network.

The elements of Figure 3–4 are defined in Table 3–1.

Table 3–1 Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST1	bond0	192.168.10.1/255.255.224.0		IPoIB/ Fixed	ComputNode1/IAMHOST1	NA	Access to IAMHOST1 using the internal IPoIB network.

Table 3–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST2	bond0	192.168.10.2/255.255.224.0		IPoIB/ Fixed	ComputNode2/IAMHOST2	NA	Access to IAMHOST2 using the internal IPoIB network.
OTDADMINVHN	bond1:1	10.10.30.1/255.255.224.0		EoIB /Floating	ComputNode1/IAMHOST1	OTD Administration Server	A floating IP address for the Administration Server is recommended, if you want to manually migrate the OTD Administration Server from IAMHOST1 to IAMHOST2.
IADADMINVHN	bond1:2	10.10.30.2/255.255.224.0		EoIB /Floating	ComputNode2/IAMHOST1	IAMAccessDomain Administration Server	A floating IP address for the IAMAccessDomain Administration Server is recommended, if you want to manually migrate the Administration Server from IAMHOST1 to IAMHOST2.

Table 3–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IGDADMINVHN	bond1:3	10.10.30.3/255.255.224.0		EoIB /Floating	ComputNode1/IAMHOST1	IAMGovernanceDomain Administration Server	A floating IP address for the IAMGovernanceDomain Administration Server is recommended, if you want to manually migrate the Administration Server from IAMHOST1 to IAMHOST2.
WEBHOST1VHN	OTD	10.10.50.1/255.255.224.0		EoIB /Floating	ComputNode1/IAMHOST1	OTD - IAMHOST1	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect. This is recommended but optional.
WEBHOST2VHN	OTD	10.10.50.2/255.255.224.0		EoIB /Floating	ComputNode2/IAMHOST2	OTD - IAMHOST2	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect. This is recommended but optional

Table 3–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST1VHN1	bond0:1	192.168.30.1/255.255.240.0		IPoIB/Floating	ComputNode1/IAMHOST1	WLS_OIM1 Default Channel	Initially enabled in IAMHOST 1 can be failed over by server migration to IAMHOST 2.
OIMHOST2VHN1	bond0:1	192.168.30.2/255.255.240.0		IPoIB/Floating	ComputNode2/IAMHOST2	WLS_OIM2 Default Channel	Initially enabled in IAMHOST 2 can be failed over by server migration to IAMHOST 1.
OIMHOST1VHN2	bond0:2	192.168.30.3/255.255.240.0		IPoIB/Floating	ComputNode1/IAMHOST1	WLS_SOA1 default channel	Initially enabled in IAMHOST 1 can be failed over by server migration to IAMHOST 2.
OIMHOST2VHN2	bond0:2	192.168.30.4/255.255.240.0		IPoIB/Floating	ComputNode2/IAMHOST2	WLS_SOA2 default channel	Initially enabled in IAMHOST 2 can be failed over by server migration to IAMHOST 1.
OIMHOST1VHN3	bond0:3	192.168.30.5/255.255.240.0		IPoIB/Floating	ComputeNode1/IAMHOST1	WLS_BI1 default channel	Initially enabled in IAMHOST 2 can be failed over by server migration to IAMHOST 1

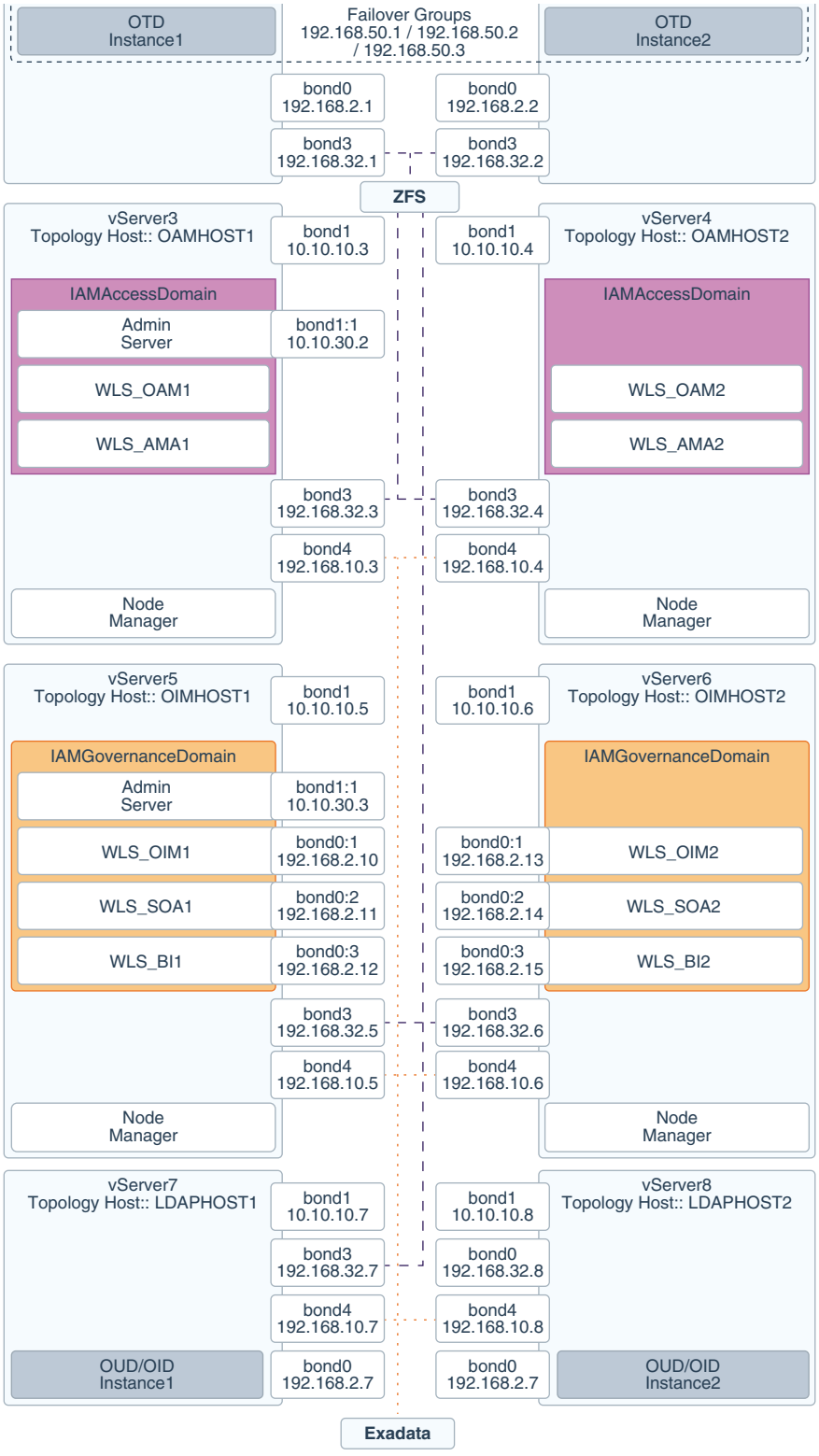
Table 3–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST2VHN3	bond0:3	192.168.30.6/255.255.240.0		IPoIB/Floating	ComputeNode2/IAMHOST2	WLS_BI1 default channel	Initially enabled in IAMHOST1 can be failed over by server migration to IAMHOST2
IAMHOST1EXT	bond1	10.10.10.1/255.255.240.0		EoIB/Fixed	ComputNode1/IAMHOST1	NA	A fixed IP allowing the compute node to be accessed by an External Corporate Network (EoIB)
IAMHOST2EXT	bond1	10.10.10.2/255.255.240.0		EoIB/Fixed	ComputNode2/IAMHOST2	NA	A fixed IP allowing the compute node to be accessed by an External Corporate Network (EoIB)
IGDINTERNAL	OTD	192.168.50.1/255.255.224.0		IPoIB/Floating	ComputNode1/IAMHOST1	NA	Oracle Traffic Director failover group for SOA
IADINTERNAL	OTD	192.168.50.2/255.255.224.0		IPoIB/Floating	ComputNode2/IAMHOST2	NA	Oracle Traffic Director failover group for MSM
IDSTORE	OTD	192.168.50.3/255.255.224.0		IPoIB/Floating	ComputNode2/IAMHOST2	NA	Oracle Traffic Director failover group for LDAP

3.4.2.2 Virtual Exalogic

Figure 3–5 shows the typical network map for an Identity and Access Management deployment on a virtual Exalogic environment.

Figure 3–5 Virtual Exalogic Network Map



If you are not using an external Web tier, you can configure all components to use the Internal IPoIB network. Oracle traffic Director and MSAS are configured to accept requests on the EoIB network, but pass them on to WebLogic and LDAP using the IPoIB network.

The elements of Figure 3–5 are defined in Table 3–2.

Table 3–2 Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
WEBHOST1	bond0	192.168.2.1/255.255.224.0		IPoIB/Fixed	vServer1/WEBHOST1	NA	Access to vServer11/WEBHOST1 via the internal IPoIB network.
WEBHOST2	bond0	192.168.2.2/255.255.224.0		IPoIB/Fixed	vServer2/WEBHOST2	NA	Access to vServer2/WEBHOST2 via the internal IPoIB network.
OAMHOST1	bond0	192.168.2.3/255.255.224.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	Access to vServer3/OAMHOST1 via the internal IPoIB network
OAMHOST2	bond0	192.168.2.4/255.255.224.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	Access to vServer4/OAMHOST2 via the internal IPoIB network
OIMHOST1	bond0	192.168.10.5/255.255.224.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	Access to vServer5/OIMHOST1 via the internal IPoIB network
OIMHOST2	bond0	192.168.10.6/255.255.224.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	Access to vServer6/OIMHOST2 via the internal IPoIB network
LDAPHOST1	bond0	192.168.10.7/255.255.224.0		IPoIB/Fixed	vServer7/LDAPHOST1	NA	Access to vServer7/LDAPHOST1 via the internal IPoIB network
LDAPHOST2	bond0	192.168.10.8/255.255.224.0		IPoIB/Fixed	vServer8/LDAPHOST2	NA	Access to vServer8/LDAPHOST2 via the internal IPoIB network

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
OTDADMINVHN	bond1:1	10.10.30.1/255.255.224.0		EoIB/Floating	vServer1/WEBHOST1	OTD Administration Server	A floating IP address for the Administration Server is recommended, if you want to manually migrate the OTD Administration Server from WEBHOST1 to WEBHOST2.
IADADMINVHN	bond1:1	10.10.30.2/255.255.224.0		EoIB/Floating	vServer3/OAMHOST1	IAMAccessDomain Administration Server	A floating IP address for the IAMAccessDomain Administration Server is recommended, if you want to manually migrate the Administration Server from OAMHOST1 to OAMHOST2.
IGDADMINVHN	bond1:1	10.10.30.3/255.255.224.0		EoIB/Floating	vServer5/OIMHOST1	IAMGovernanceDomain Administration Server	A floating IP address for the IAMGovernanceDomain Administration Server is recommended, if you want to manually migrate the Administration Server from OIMHOST2 to OIMHOST1
WEBHOST1VHN1	OTD	10.10.50.1/255.255.224.0		EoIB/Floating	vServer1/WEBHOST1	OTD - WEBHOST1	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect. This is optional

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
WEBHOST2VHN1	OTD	10.10.50.2/255.255.224.0		EoIB/Floating	vServer2/WEBHOST2	OTD - WEBHOST2	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect. This is optional.
OIMHOST1VHN1	bond0:1	192.168.30.1/255.255.240.0		IPoIB/Floating	vServer5/OIMHOST1	WLS_OIM1 Default Channel	Initially enabled in OIMHOST1 and can be failed over by server migration to OIMHOST2
OIMHOST2VHN1	bond0:1	192.168.30.2/255.255.240.0		IPoIB/Floating	vServer6/OIMHOST2	WLS_OIM2 Default Channel	Initially enabled in OIMHOST2 and can be failed over by server migration to OIMHOST1
OIMHOST1VHN2	bond0:2	192.168.30.3/255.255.240.0		IPoIB/Floating	vServer5/OIMHOST1	WLS_SOA1 Default Channel	Initially enabled in OIMHOST1 and can be failed over by server migration to OIMHOST2
OIMHOST2VHN2	bond0:2	192.168.30.4/255.255.240.0		IPoIB/Floating	vServer6/OIMHOST2	WLS_SOA2 Default Channel	Initially enabled in OIMHOST2 and can be failed over by server migration to OIMHOST1.
OIMHOST1VHN3	bond0:3	192.168.30.5/255.255.224.0		IPoIB/Floating	vServer5/OIMHOST1	WLS_BI1 Default Channel	Initially enabled in OIMHOST1 and can be failed over by server migration to OIMHOST2.

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST2VHN3	bond0:3	192.168.30.6/255.255.224.0		IPoIB/Floating	vServer6/OIMHOST2	WLS_BI2 Default Channel	Initially enabled in OIMHOST2 and can be failed over by server migration to OIMHOST1.
WEBHOST1-EXT	bond1	10.10.10.1/255.255.240.0		EoIB/Fixed	vServer1/WEBHOST1	NA	A fixed IP allowing the vServer to be accessed by an External Load balancer
WEBHOST2-EXT	bond1	10.10.10.2/255.255.240.0		EoIB/Fixed	vServer2/WEBHOST2	NA	A fixed IP allowing the vServer to be accessed by an External Load balancer
WEBHOST1-STOR	bond3	192.168.32.1/255.255.240.0		IPoIB/Fixed	vServer1/WEBHOST1	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
WEBHOST2-STOR	bond3	192.168.32.2/255.255.240.0		IPoIB/Fixed	vServer2/WEBHOST2	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
OAMHOST1-STOR	bond3	192.168.32.3/255.255.240.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
OAMHOST2-STOR	bond3	192.168.32.4/255.255.240.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
OIMHOST1-STOR	bond3	192.168.32.5/255.255.240.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
OIMHOST2-STOR	bond3	192.168.32.6/255.255.240.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
LDAPHOST1-STOR	bond3	192.168.32.7/255.255.240.0		IPoIB/Fixed	vServer7/LDAPHOST1	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.
LDAPHOST2-STOR	bond3	192.168.32.8/255.255.240.0		IPoIB/Fixed	vServer8/LDAPHOST2	NA	A fixed IP address allowing the vServer to connect to the ZFS Storage appliance using the internal network.

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
OAMHOST1-DATA	bond4	192.168.10.3/255.255.240.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OAMHOST2-DATA	bond4	192.168.10.4/255.255.240.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OIMHOST1-DATA	bond4	192.168.10.5/255.255.240.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OIMHOST2-DATA	bond4	192.168.10.6/255.255.240.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
LDAPHOST1-DATA	bond4	192.168.10.7/255.255.240.0		IPoIB/Fixed	vServer7/LDAPHOST1	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.

Table 3–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

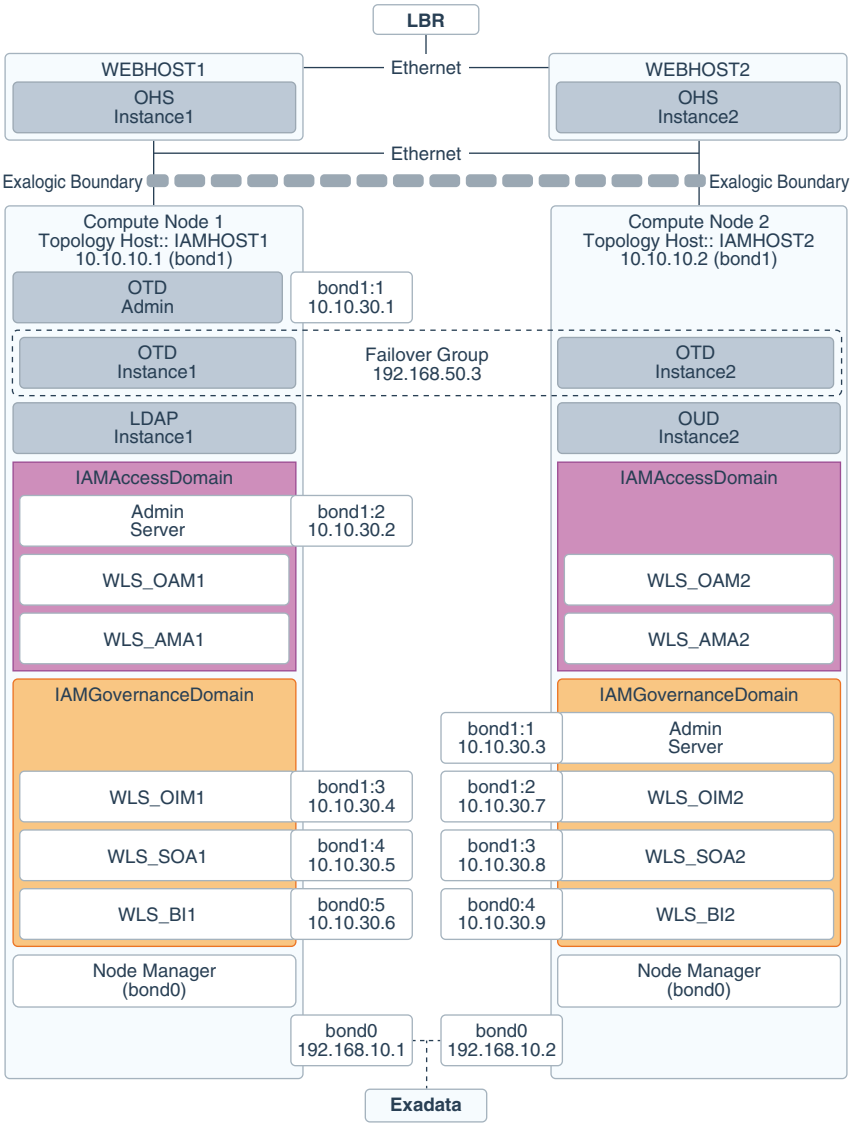
Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
LDAPHOST2-DATA	bond4	192.168.10.8/255.255.240.0		IPoIB/Fixed	vServer8/LDAPHOST2	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
IGDINTERNAL	OTD	192.168.50.1/255.255.224.0		IPoIB/Floating	vServer1/WEBHOST1	NA	Oracle Traffic Director failover group for SOA
IADINTERNAL	OTD	192.168.50.2/255.255.224.0		IPoIB/Floating	vServer2/WEBHOST2	NA	Oracle Traffic Directory Group for MSM
IDSTORE	OTD	192.168.50.3/255.255.224.0		IPoIB/Floating	vServer2/WEBHOST2	NA	Oracle Traffic Director failover group for LDAP.

Note: The IP addresses listed in Table 3–2 are for example only. Because of the way that IP addresses are allocated in virtual Exalogic, it is highly unlikely that you will be able to use the exact values in this table.

3.4.2.3 Physical Exalogic with External Web Tier

Figure 3–6 shows the typical network map for an Identity and Access Management deployment on a physical Exalogic environment with external Web Tier.

Figure 3–6 Physical Exalogic Network Map



If you are not using an external Web tier, you can configure all components to use the Internal IPoIB network. Oracle traffic Director and MSAS are configured to accept requests on the EoIB network, but pass them on to WebLogic and LDAP using the IPoIB network.

The elements of Figure 3–6 are defined in Table 3–3.

Table 3–3 Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST1	bond0	192.168.10.1/255.255.224.0		IPoIB/Fixed	ComputNode1/IAMHOST1	NA	Access to IAMHOST1 using the internal IPoIB network.

Table 3–3 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST2	bond0	192.168.10.2/255.255.224.0		IPoIB/Fixed	ComputNode2/IAMHOST2	NA	Access to IAMHOST2 using the internal IPoIB network.
OTDADMINVHN	bond1:1	10.10.30.1/255.255.224.0		EoIB/Floating	ComputNode1/IAMHOST1	OTD Administration Server	A floating IP address for the Administration Server is recommended, if you want to manually migrate the OTD Administration Server from IAMHOST1 to IAMHOST2.
IADADMINVHN	bond1:2	10.10.30.2/255.255.224.0		EoIB/Floating	ComputNode2/IAMHOST1	IAMAccessDomain Administration Server	A floating IP address for the IAMAccessDomain Administration Server is recommended, if you want to manually migrate the Administration Server from IAMHOST1 to IAMHOST2.
IGDADMINVHN	bond1:1	10.10.30.3/255.255.224.0		EoIB/Floating	ComputNode1/IAMHOST1	IAMGovernanceDomain Administration Server	A floating IP address for the IAMGovernanceDomain Administration Server is recommended, if you want to manually migrate the Administration Server from IAMHOST1 to IAMHOST2.

Table 3–3 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST1VHN1	bond1:3	10.10.30.4/255.255.240.0		EoIB/Floating	ComputNode1/IAMHOST1	WLS_OIM1 Default Channel	Initially enabled in IAMHOST1 can be failed over by server migration to IAMHOST2.
OIMHOST2VHN1	bond1:2	10.10.30.7/255.255.240.0		EoIB/Floating	ComputNode2/IAMHOST2	WLS_OIM2 Default Channel	Initially enabled in IAMHOST2 can be failed over by server migration to IAMHOST1.
OIMHOST1VHN2	bond1:4	10.10.30.5/255.255.240.0		EoIB/Floating	ComputNode1/IAMHOST1	WLS_SOA1 default channel	Initially enabled in IAMHOST1 can be failed over by server migration to IAMHOST2.
OIMHOST2VHN2	bond0:3	10.10.30.8/255.255.240.0		EoIB/Floating	ComputNode2/IAMHOST2	WLS_SOA2 default channel	Initially enabled in ComputeNode3 can be failed over by server migration to IAMHOST1.
OIMHOST1VHN3	bond1:5	10.10.30.6/255.255.224.0		EoIB/Floating	ComputNode1/IAMHOST1	WLS_BI1 Default Channel	Initially enabled in IAMHOST1 can be failed over by server migration to IAMHOST2.
OIMHOST2VHN3	bond1:4	10.10.30.9/255.255.224.0		EoIB/Floating	ComputNode2/IAMHOST2	WLS_BI1 Default Channel	Initially enabled in IAMHOST2 can be failed over by server migration to IAMHOST1.
IAMHOST1-EXT	bond1	10.10.10.1/255.255.240.0		EoIB/Fixed	ComputNode1/IAMHOST1	NA	A fixed IP allowing the compute node to be accessed by an External Load balancer

Table 3–3 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address/Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST2-EXT	bond1	10.10.10.2/255.255.240.0		EoIB/Fixed	ComputNode2/IAMHOST2	NA	A fixed IP allowing the compute node to be accessed by an External Load balancer
IDSTORE	OTD	192.168.50.3/255.255.224.0		IPoIB/Floating	ComputNode2/IAMHOST2	NA	Oracle Traffic Director failover group for Oracle Unified Directory

3.4.3 Summary of Oracle Identity and Access Management Load Balancing Virtual Server Names

In order to distribute requests equally between servers, and to provide high availability, a hardware load balancer is required. The hardware load balancer should exist on redundant hardware to ensure maximum availability. The hardware load balancer is configured to recognize a set of virtual server names.

If you have configured your Exalogic appliance so that all traffic is using the EoIB network, your load balancer can be configured the same way as platform deployments. However, a better approach on Exalogic is to use Oracle Traffic Director for load balancing between internal components.

For information about the purpose of these server names, see Section 1.2.3.2, "Summary of the Typical Load Balancer Virtual Server Names."

The hardware load balancer in Oracle Identity and Access Management deployments recognizes the following virtual server names.

- login.example.com - This virtual server name is used for all incoming access traffic. It acts as the access point for all HTTP traffic to the runtime Access Management components. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  ```
  login.example.com:443
  ```

  If you are using an external Web tier, this virtual host distributes requests among the external Web servers. Otherwise, it distributes requests between the internal Oracle Traffic Director servers.

- prov.example.com - This virtual server name is used for all incoming governance traffic. It acts as the access point for all HTTP traffic to the runtime Access Management components. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  ```
  prov.example.com:443
  ```

If you are using an external Web tier, this virtual host distributes requests between the external Web servers. Otherwise, it distributes requests between the internal Oracle Traffic Director servers.

In previous releases of the Enterprise Deployment Guide login.example.com and prov.example.com were the same entry point. This release allows for them to be separated out. This will enable smarter routing from the load balancer, allow a more modular deployment and will facilitate future Multi-datacenter deployments. If desired these two entry points can still be combined to provide a single point of entry into the IAM deployment.

- msas.example.com - This virtual server name is used for all incoming Mobile Security traffic. It acts as the access point for all HTTPS traffic to the runtime Mobile Security Access Service. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  ```
  msas.example.com:9002
  ```

  If you are using an external web tier, then this virtual host will distribute requests amongst the external MSAS servers, otherwise it will distribute requests amongst the internal MSAS servers.

- iadadmin.example.com - This virtual server name is for internal communications between the application tier components in the Access Domain only and is not exposed to the Internet. The primary use of this virtual server is to allow the Mobile Security Access Service to communicate with either the Oracle HTTP server, which is being used to distribute requests to Oracle Mobile Security Manager, or it can be used to send requests directly to the WebLogic Managed Servers hosting Mobile Security Manager.

  The traffic from clients to this URL is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  ```
  iadadmin.example.com:80
  ```

  If you are not using external Web Servers, then this virtual host can be configured on Oracle Traffic Director rather than the hardware load balancer.

- igdadmin.example.com - This virtual server name is for internal communications between the application tier components in the Governance Domain only and is not exposed to the Internet. The services accessed on this virtual host include the WebLogic Administration Server Console, Oracle Enterprise Manager Fusion Middleware Control, and Identity Manager System Administration console.

  The traffic from clients to this URL is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  ```
  igdadmin.example.com:80
  ```

  If you are not using external Web Servers, this virtual host can be configured on Oracle Traffic Director rather than the hardware load balancer.

- igdinternal.example.com - This virtual server name is for internal communications between the application tier components in the Governance domain only and is not exposed to the Internet. Specifically, for the Oracle Identity and Access Management enterprise topology, this URL is used for both Oracle OIM Suite and Oracle SOA Suite internal communications.

The traffic from clients to this URL is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

```
igdinternal.example.com:7777
```

If you are not using external Web Servers, then this virtual host can be configured on Oracle Traffic Director rather than the hardware load balancer.

- iadinternal.example.com - This virtual server name is for internal communications between the application tier components in the Access domain only and is not exposed to the Internet. Specifically, for the Oracle Identity and Access Management enterprise topology, this URL is used by the Mobile Security Access Server to callback to Oracle Mobile Security Manager.

  The traffic from clients to this URL is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  ```
  iadinternal.example.com:7777
  ```

  If you are not using external Web Servers, this virtual host can be configured on Oracle Traffic Director rather than the hardware load balancer.

- idstore.example.com - This virtual server name is used for all incoming identity store traffic. It acts as the access point to the LDAP directory instances. This virtual server is not exposed to the Internet.

  The traffic from clients to this URL is may or may not be SSL-enabled, depending on the type of LDAP directory in use, typically this is non-SSL enabled for Oracle Unified Directory and Oracle Internet Directory and enabled for Microsoft Active Directory. Clients access this service using the following address and the requests are forwarded to the LDAP instances.

  This virtual host is configured on Oracle Traffic Director rather than the hardware load balancer.

3.5 Summary of the Managed Servers and Clusters on the Application Tier Hosts

The Application tier hosts the Administration Server and Managed Servers in the Oracle WebLogic Server domains.

Depending upon the components you select, the Oracle WebLogic Server domain for the Oracle Identity and Access Management consists of the clusters shown in Table 3–4. These clusters function as active-active high availability configurations.

Table 3–4 Summary of Managed Servers and CLusters

Domain	Cluster	Managed Servers
IAMAccessDomain	Oracle Access Manager	wls_oam1, wls_oam2
	Oracle Policy Manager	wls_ama1, wls_ama2
	Oracle Mobile Security Manager	wls_msm1, wls_msm2
IAMGovernanceDomain	Oracle Identity Manager	wls_oim1, wls_oim2
	Oracle SOA Suite	wls_soa1, wls_soa2
	Oracle Business Intelligence	wls_bi1, wls_bi2

Depending upon the components you select, the Oracle WebLogic Server domain for the Oracle Identity and Access Management consists of the clusters shown in …. These clusters function as active-active high availability configurations.

3.6 Understanding Oracle Traffic Director

Oracle Traffic Director (OTD) serves as a load balancer and a Web router. OTD is not a fully functional Web server, but can perform many tasks that a Web server performs. It is made up of an administration server, instances, and Failover Groups.

For information about installing and configuring Oracle Traffic Director, see Section 14.2, "Configuring Oracle Traffic Director."

This section contains the following topics

- Section 3.6.1, "About Oracle Traffic Director in a Standard Exalogic Deployment."
- Section 3.6.2, "About Oracle Traffic Director in a Deployment with Oracle HTTP Server."
- Section 3.6.3, "About Oracle Traffic Director Failover Groups."
- Section 3.6.4, "About Oracle Traffic Director and the Load Balancer."
- Section 3.6.5, "About Oracle Traffic Director and Identity and Access Management."

3.6.1 About Oracle Traffic Director in a Standard Exalogic Deployment

Oracle Traffic Director is supported only with Exalogic deployments. It is used to load balance requests to:

- LDAP - Manage a Virtual IP Address that internal servers can access for the purposes of making LDAP calls.

  Receive requests on the LDAP Virtual IP address and pass them on to the running LDAP instances using the IPoIB Network

- Internal call backs - Manage a Virtual IP Address that internal servers can access for the purposes of making Inter application call backs

  Receive requests on the Callback Virtual IP address and pass them on to the appropriate Weblogic Managed Servers using the IPoIB Network

The hardware load balancer sends requests to Oracle Traffic Director.

Oracle Traffic Director receives requests from the Load balancer and from internal applications requiring access to other internal applications or LDAP. Upon receipt of these requests, Oracle Traffic Director forwards them on to WebLogic Managed Servers or LDAP.

For more information about the standard Exalogic topology described in this guide, see Section 3.3, "Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies."

3.6.2 About Oracle Traffic Director in a Deployment with Oracle HTTP Server

Oracle Traffic Director is supported only with Exalogic deployments. It is used to load balance requests to:

- LDAP - Receive HTTP requests from the hardware load balancer on the EoIB network and forward them on to the WebLogic Managed Servers on the IPoIB network.

  Manage a Virtual IP Address that internal servers can access for the purposes of making LDAP calls.

  Receive requests on the LDAP Virtual IP address and pass them on to the running LDAP instances using the IPoIB Network.

- Internal call backs - Manage a Virtual IP Address that internal servers can access for the purposes of making Inter application call backs.

  Receive requests on the Callback Virtual IP address and pass them on to the appropriate Weblogic Managed Servers using the IPoIB Network.

A hardware load balancer sends requests to Oracle HTTP Server (OHS), which resides on commodity servers on the corporate ethernet network. The OHS then passes these requests onto WebLogic servers using the EoIB network.

3.6.3 About Oracle Traffic Director Failover Groups

Oracle Traffic Director manages floating IP addresses for LDAP and internal callbacks on the IPoIB network. When a failover group is created, you specify the IP address netmasks you wish to use for a primary node and a failover node. It uses a heartbeat between instances to detect a failure.

For information about creating and configuring failover groups, see Section 14.2.10, "Creating a Failover Group for Virtual Hosts."

3.6.4 About Oracle Traffic Director and the Load Balancer

You can configure the load balancer to point to Oracle Traffic Director instances. However, the load balancer failure detection is slower than using OTD failover groups. Therefore, Oracle recommends creating an external failover group for each Oracle Traffic Director instance and pointing the load balancer to the failover groups.

3.6.5 About Oracle Traffic Director and Identity and Access Management

Oracle Traffic Director has its own WebGate, which is used for authentication. After WebGate is installed and configured, Oracle Traffic Director intercepts requests for the consoles and forwards them to Access Manager for validation.

Internal callbacks go back to failover groups to make efficient use of the Infiniband network.

3.7 About Exalogic Optimizations for WebLogic

Exalogic offers the following optimizations for WebLogic:

Domain Level:

- Check box in WebLogic Domain
- Increased Network IO
- Increased efficiency in session replication
- Self-tuning thread pool

Cluster Level:

Creates a custom network replication channel for improved network throughput.

For more information about, and procedures for Exalogic Optimization see "WebLogic Server Domain Optimizations for Exalogic Elastic Cloud Software" in *Administering WebLogic Server for Oracle Exalogic Elastic Cloud*.

3.8 Roadmap for Implementing the Primary Oracle Identity and Access Management Topologies

Table 3–5 provides a roadmap for implementing the primary IAM suite topologies on Exalogic.

Table 3–5 Roadmap for Implementing Primary IAM Suite Topologies on Exalogic

Scenario	Tasks	For More Information, See
Creating an IAM Enterprise Deployment manually on Exalogic	Review the primary Exalogic enterprise topologies.	Section 3.3, "Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies"
	Review the hardware and software requirements and procure the resources for the enterprise deployment.	Chapter 5, "Procuring Resources for an Enterprise Deployment"
	Prepare the load balancers and firewalls.	Chapter 6, "Preparing the Load Balancer and Firewalls for an Enterprise Deployment"
	Prepare the storage and understand the directory structure.	Chapter 7, "Preparing Storage for an Enterprise Deployment"
	Prepare the Exalogic machine.	Chapter 8, "Preparing Exalogic for an Oracle Identity and Access Management Deployment"
	Configure the host computers.	Chapter 9, "Configuring the Host Computers for an Enterprise Deployment"
	Prepare the database.	Chapter 10, "Preparing the Database for an Enterprise Deployment"
	Install the required softwares.	Chapter 11, "Installing Oracle Fusion Middleware in Preparation for an Enterprise Deployment"
	Configure Oracle LDAP.	Chapter 12, "Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment"
	Prepare the identity store.	Chapter 13, "Preparing The Identity Store"
	Configure the Oracle Web Tier.	Chapter 14, "Configuring the Oracle Web Tier"
	Create the WebLogic domains.	Chapter 15, "Creating Domains for an Enterprise Deployment"
	Set up the Node Manager.	Chapter 16, "Setting Up Node Manager for an Enterprise Deployment"
	Configure Oracle Access Management (OAM).	Chapter 17, "Configuring Oracle Access Management"
	Configure Oracle Mobile Security Services (OMSS).	Chapter 18, "Configuring Oracle Mobile Security Services"
	Configure Oracle Identity Manager (OIM).	Chapter 19, "Configuring Oracle Identity Manager"
	Configure Oracle BI Publisher (BIP).	Chapter 20, "Configuring BI Publisher"
	Configure server migration settings.	Chapter 21, "Configuring Server Migration for an Enterprise Deployment"

Table 3–5 (Cont.) Roadmap for Implementing Primary IAM Suite Topologies on Exalogic

Scenario	Tasks	For More Information, See
Creating an IAM Enterprise Deployment using Life Cycle Management Tools (IDMLCM), on Exalogic	Understand the automated deployment process.	Chapter 23, "Introduction to the Life Cycle Management (LCM) Tools"
	Prepare the Exalogic machine.	Chapter 8, "Preparing Exalogic for an Oracle Identity and Access Management Deployment"
	Install the Oracle Identity and Access Management Life Cycle Management Tools.	Chapter 24, "Installing Oracle Identity and Access Management Life Cycle Management Tools"
	Create a deployment response file for the topology you are deploying.	Chapter 25, "Creating a Deployment Response File"
	Deploy Identity and Access Management.	Chapter 26, "Deploying Identity and Access Management"
	Perform the required post-deployment tasks.	Chapter 27, "Performing Post-Deployment Configuration"

3.9 Building your Own Oracle Identity and Access Management Topology

This document provides step-by-step instructions for configuring the two primary enterprise topologies for Oracle Identity and Access Management, which are described in Section 3.3, "Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies."

However, Oracle recognizes that the requirements of your organization may vary, depending on the specific set of Oracle Fusion Middleware products you purchase and the specific types of applications you deploy.

In many cases, you can install and configure an alternative topology, one that includes additional components, or one that does not include all the Oracle Identity and Access Management products shown in the primary topology diagrams.

The following sections describe some alternative Oracle Identity and Access Management topologies you can implement, using some variations of the instructions in this guide:

- OAM Only with an Existing Directory
- OIM Only with an Existing Directory
- OAM/OIM Integrated in a Modular Deployment
- OAM/OIM Integrated with an Existing Directory

Note: The deployment can be extended with Oracle Adaptive Access Manager or Oracle Privileged Account Manager. See the MAA Web site for details.

Note: if you decide to deploy a custom environment that varies from the ones provided in this guide, then you typically deploy Oracle Identity and Access Management manually. The Life Cycle Management (LCM) Tools provided to automate the installation and deployment do not support all the alternative topologies.

For information about the topologies that you can deploy using LCM Tools, see Chapter 23, "Introduction to the Life Cycle Management (LCM) Tools".

3.10 About Installing and Configuring a Custom Enterprise Topology

If you choose to implement a topology that is not described in this guide, be sure to review the certification information, system requirements, and interoperability requirements for the products you want to include in the topology.

After you verify that the topology is supported, you can either use these instructions as a guide to installing and configuring the components you need, or you can install and configure a standard installation topology using the Oracle Fusion Middleware 11g installation guides and use the "Start Small and Scale Out" approach to configuring your environment.

3.11 About Using Server Migration to Enable High Availability of the Oracle Identity and Access Management Enterprise Topology

To ensure high availability of the Oracle Access Suite products and components, this guide recommends that you enable Oracle WebLogic Server Whole Server Migration for the Oracle Identity Manager, Oracle SOA Suite, and Oracle Business Intelligence clusters that you create as part of the reference topology.

Whole server migration provides for the automatic restart of a server instance, with all of its services, on a different physical machine. When a failure occurs in a server that is part of a cluster that is configured with server migration, the server is restarted on any of the other machines that host members of the cluster.

For more information, see Chapter 21, "Configuring Server Migration for an Enterprise Deployment."

Part II

Preparing for an Enterprise Deployment

Part I contains the following chapters:

4

Using the Enterprise Deployment Workbook

This chapter introduces the Enterprise Deployment Workbook; it describes how you can use the workbook to plan an enterprise deployment for your organization.

This chapter contains the following sections:

4.1 Introduction to the Enterprise Deployment Workbook

The Oracle Fusion Middleware Enterprise Deployment Workbook is a companion document to this guide. It is a spreadsheet that can be used by architects, system engineers, database administrators, and others to plan and record all the details for the environment deployment including server names, URLs, port numbers, installation paths, and other resources.

The Enterprise Deployment Workbook serves as a single document you can use to track input variables for the entire process, allowing for:

- Separation of tasks between architects, system engineers, database administrators, and other key organizational roles
- Comprehensive planning before the implementation
- Validation of planned decisions before actual implementation
- Consistency during implementation
- A record of the environment for future use

4.2 Typical Use Case for Using the Workbook

A typical use case for the Enterprise Deployment Workbook involves the following roles and tasks, in preparation for an Oracle Fusion Middleware enterprise deployment:

- Architects read through the first five chapters of this guide, and fill in the corresponding sections of the Workbook.
- The Workbook is validated by other architects and system engineers.

- The architect uses the validated workbook to initiate network and system change requests with system engineering departments;
- The Administrators and System Integrators who are installing and configuring the software refer to the workbook and the subsequent chapters of this guide to perform the installation and configuration tasks.

4.3 Who Should Use the Enterprise Deployment Workbook?

The information in the Enterprise Deployment Workbook is divided into categories. Depending on the structure of your organization and roles defined for your team, you can assign specific individuals in your organization to fill in the details of the workbook. Similarly the information in each category can be assigned to the individual or team responsible for planning, procuring, or setting up each category of resources.

For example, the workbook can be filled in, reviewed, and used by people in your organization that fill the following roles:

- Information Technology (IT) Director
- Architect
- System Administrator
- Network Engineer
- Database Administrator
- Storage Administrator
- Fusion Middleware Administrator

4.4 Using the Oracle Identity and Access Management Enterprise Deployment Workbook

The following sections provide an introduction to the location and contents of the Oracle Identity and Access Management Enterprise Deployment Workbook:

- Section 4.4.1, "Locating the Oracle Identity and Access Management Enterprise Deployment Workbook"
- Section 4.4.2, "Understanding the Contents of the Oracle Identity and Access Management Enterprise Deployment Workbook"

4.4.1 Locating the Oracle Identity and Access Management Enterprise Deployment Workbook

The Oracle Identity and Access Management Enterprise Deployment Workbook is available as a Microsoft Excel Spreadsheet in the Oracle Fusion Middleware documentation library. It is available as a link on the Install, Patch, and Upgrade page of the library.

4.4.2 Understanding the Contents of the Oracle Identity and Access Management Enterprise Deployment Workbook

The following sections describe the contents of the Oracle Identity and Access Management Enterprise Deployment Workbook. The workbook is divided into tabs, each containing a set of related variables and values you will need to install and

configure the Oracle Identity and Access Management Enterprise Deployment topologies:

- Section 4.4.2.1, "Using the Start Tab"
- Section 4.4.2.2, "Using the Hardware - Host Computers Tab"
- Section 4.4.2.3, "Using the Network - Virtual Hosts & Ports Tab"
- Section 4.4.2.4, "Using the Load Balancer Tab"
- Section 4.4.2.5, "Using the Storage - Directory Variables Tab"
- Section 4.4.2.6, "Using the Database - Connection Details Tab"
- Section 4.4.2.7, "Using the LDAP - Users and Groups Tab"
- Section 4.4.2.8, " Using the Exalogic Tab"

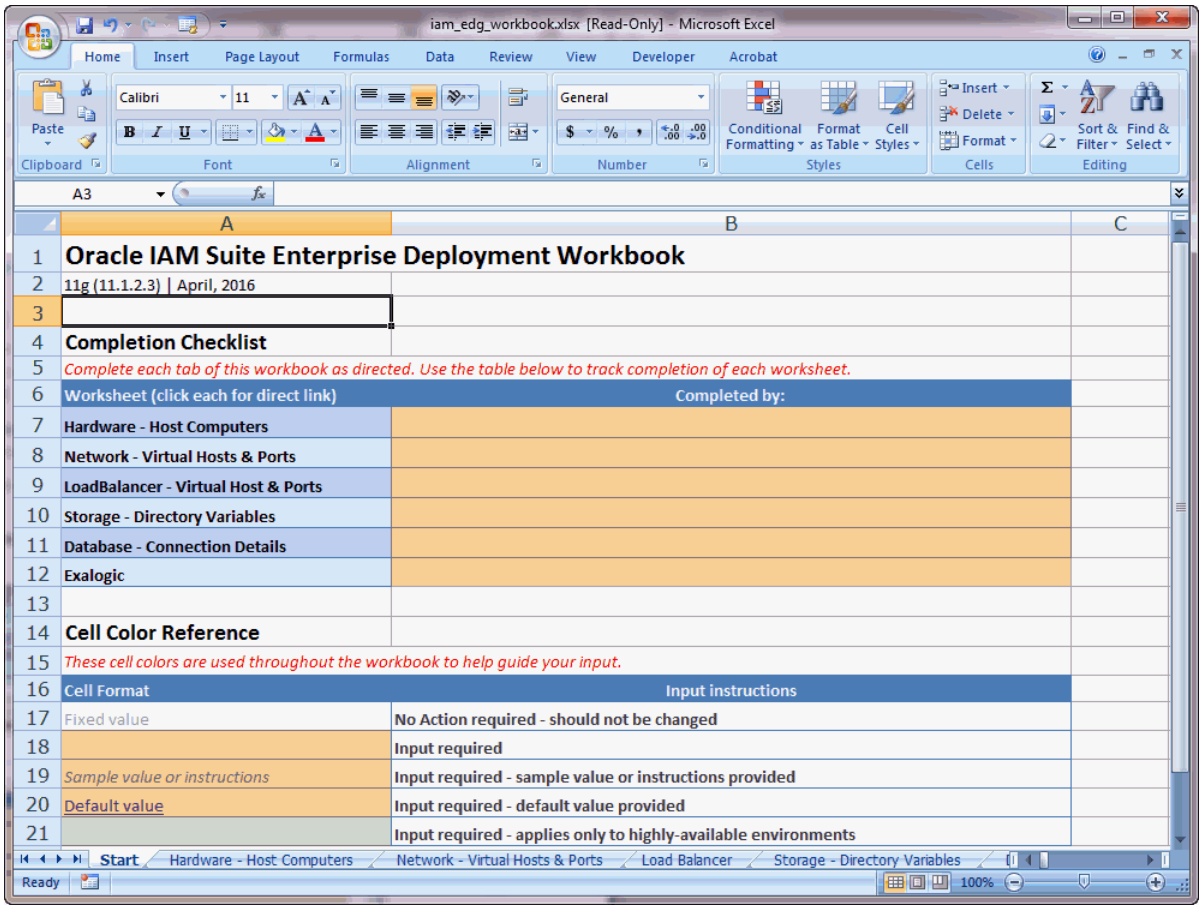
4.4.2.1 Using the Start Tab

The Start tab of the Enterprise Deployment Workbook serves as a table of contents for the rest of the workbook. You can also use it to identify the people who will be completing the spreadsheet.

The Start tab also provides a key to identify the colors used to identify workbook fields that need values, as well as those that are provided for informational purposes.

Figure 4–1 shows the Start tab of the spreadsheet.

Figure 4–1 Start Tab of the Oracle Identity and Access Management Enterprise Deployment Workbook



4.4.2.2 Using the Hardware - Host Computers Tab

The Hardware - Host Computers tab lists the host computers required to install and configure the Oracle Identity and Access Management Enterprise Deployment Topology.

The reference topologies described in Section 2.1, "Understanding the Primary and Build-Your-Own Enterprise Deployment Topologies" require a minimum of six host computers: two for the Web tier, two for the application tier, and two for the Oracle RAC database on the data tire.

A common deployment model typically uses 10 servers however. These being made up of: 2 for the Web Tier, 2 for the Access Components Application Tier, 2 for the Governance Components Application Tier, 2 For the LDAP servers and 2 for the RAC database servers. If you decide to expand the environment to include more systems, add a row for each additional host computer.

The **Abstract Host Name** is the name used throughout this guide to reference the host. For each row, procure a host computer, and enter the **Actual Host Name**.

For example, if a procedure in this guide references OAMHOST1, you can then replace the OAMHOST1 variable with the actual name provided on the **Hardware - Host Computers** tab of the workbook.

About Multi-Networked Host Computers

If you are deploying on a multi-networked host, the real host name may not be attached to the network on which you wish communication to occur. If the network you wish to use for communication is different from that attached to the **Real Host Name**, then you can override this by providing a different **Listen Address Host Name**, which is attached to the network you wish to use. Most platform deployments do not require a different **Listen Host Name**, however the majority of Exalogic Deployments do.

A typical example would be where the real host name is attached to the management network but network communication should happen through a client network or in the case of Exalogic the internal IPoIB network.

Using the Spreadsheet in a Consolidated Deployment

If you are using a consolidated deployment, where you have larger machines, then you can use the same host name for multiple entries in the spreadsheet.

For example, if you wish to deploy Access and Governance onto the same host then both OAMHOST1 and OIMHOST1 can be set to *iamserver1*, and both OAMHOST1 and OIMHOST2 can be set to *iamserver2*.

When you see OAMHOST1 or OIMHOST2 referenced in the guide, you'll know to replace them with the value of *iamserver1* or *iamserver2*.

Including Additional Host Details

For easy reference, Oracle also recommends that you include the IP address, Operating System (including the version), number of CPUs, and the amount of RAM for each host. This information can be useful during the installation, configuration, and maintenance of the enterprise deployment.

For more information, see Chapter 9, "Configuring the Host Computers for an Enterprise Deployment."

4.4.2.3 Using the Network - Virtual Hosts & Ports Tab

The Network - Virtual Hosts & Ports tab lists the virtual hosts that must be defined by your network administrator before you can install and configure the Oracle Identity and Access Management enterprise deployment topology.

The port numbers are important for several reasons. You must have quick reference to the port numbers so you can access the management consoles; the firewalls must also be configured to allow network traffic via specific ports.

Each virtual host, virtual IP address, and each network port serves a distinct purpose in the deployment. For more information, see Section 5.3, "Reserving the Required IP Addresses for an Enterprise Deployment"

In the Physical Network - Virtual Hosts table, review the items in the **Abstract Virtual Host or Virtual IP Name** column. These are the virtual host and virtual IP names used in the procedures in this guide. For each abstract name, enter the actual virtual host name defined by your network administrator. Whenever this guide references one of the abstract virtual host or virtual IP names, replace that value with the actual corresponding value in this table.

Similarly, in many cases, this guide assumes you are using default port numbers for the components or products you install and configure. However, in reality, you will likely have to use different port numbers. Use the Network - Port Numbers table to map the default port values to the actual values used in your specific installation.

4.4.2.4 Using the Load Balancer Tab

The Load Balancer tab lists the virtual hosts your network administrator must create on your hardware load balancer before you can install and configure the Oracle IAM enterprise deployment topology.

The ports you specify in this section are the ports on the load balancer. They need not be the same as the target ports you are directing traffic to.

Each virtual host, virtual IP address, and each network port serves a distinct purpose in the deployment. For more information, see Chapter 6.1.4, "Summary of the Virtual Servers Required for an Oracle Identity and Access Management Deployment."

The Virtual Hosts are separated out to provide maximum flexibility. It is however acceptable to combine the multiple virtual hosts of the same type.

In the **Load Balancer - Virtual Hosts** table, review the items in the **Abstract Virtual Host** or **Virtual IP Name** column. These are the virtual host and virtual IP names used in the procedures in this guide. For each abstract name, enter the actual virtual host name defined by your network administrator. Whenever this guide references one of the abstract virtual host or virtual IP names, replace that value with the actual corresponding value in this table.

Similarly, in many cases, this guide assumes you are using default port numbers for the components or products you install and configure. However, in reality, you will likely have to use different port numbers. Use the **Load Balancer - Port Numbers** table to map the default port values to the actual values used in your specific installation.

The Load Balancer Pool configuration combines information that you enter in this tab with information entered in the **Hardware** and **Network** tabs to provide a summary of how the load balancer pools should be configured. For full details on how to configure the load balancer refer to Chapter 6.1.2, "Typical Procedure for Configuring the Hardware Load Balancer."

4.4.2.5 Using the Storage - Directory Variables Tab

As part of preparing for an enterprise deployment, it is assumed you will be using a standard directory structure, which is recommended for Oracle enterprise deployments.

In addition, procedures in this book reference specific directory locations. Within the procedures, each directory is assigned a consistent variable, which you should replace with the actual location of the directory in your installation.

For each of the directory locations listed on this tab, provide the actual directory path in your installation.

In addition, for the application tier, it is recommended that many of these standard directories be created on a shared storage device. For those directories, the table also provides fields so you can enter the name of the shared storage location and the mount point used when you mounted the shared location.

For more information, see Chapter 7, "Preparing Storage for an Enterprise Deployment."

4.4.2.6 Using the Database - Connection Details Tab

When you are installing and configuring the enterprise deployment topology, you will often have to make connections to a highly available Oracle Real Application Clusters (RAC) database. In this guide, the procedures reference a set of variables that identify the information you will need to provide to connect to the database from tools, such as the Configuration Wizard and the Repository Creation Utility.

To be sure you have these values handy, use this tab to enter the actual values for these variables in your database installation.

An Oracle Identity and Access Management installation can use more than one database if desired. This is typically the case where you wish to use a Multi Data Center deployment. It is perfectly acceptable however, to use a single database.

If you are using a single database, you must still use a different RCU prefix for artefacts belonging to each separate domain Access and Governance.

For more information, see Chapter 10, "Preparing the Database for an Enterprise Deployment."

4.4.2.7 Using the LDAP - Users and Groups Tab

Oracle Fusion Middleware products require an LDAP directory service, such as Oracle Unified Directory. The enterprise deployment requires that you define specific users and groups in the directory, so administrators can access the management consoles and other resources required to configure and manage the deployment.

Throughout this guide, variables are used to identify these specific users and groups. Use the **LDAP - Users and Groups** tab in the enterprise deployment workbook to track these variables and the actual user and groups names used in your specific LDAP directory.

For information about configuring the LDAP directory, see the following topics:

- Chapter 12, "Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment"
- Chapter 13, "Preparing The Identity Store"

4.4.2.8 Using the Exalogic Tab

The **Exalogic** tab is relevant only if you are deploying your Enterprise Deployment on Exalogic.

While this guide covers the setup of Fusion Middleware for Exalogic, it does not cover the actual setup of the Exalogic servers. You use this section of the worksheet to determine how you need your Exalogic Environment Setup (or to record how you have actually set it up).

The page is divided into several sections:

- **Compute Node Details**: This section is required if you are performing a physical Exalogic deployment. Here you enter the names of the Hosts associated with each of the networks you wish to use.
- **Virtual Server Details**: This section is required if you are performing a virtual Exalogic deployment. Here you enter the details of the Virtual Servers you require creating on the Exalogic Elastic Cloud environment. You include such things as the size of the virtual server, the host names associated with the various Exalogic networks and the Distribution Groups.

  For a complete explanation of these items refer to the *Oracle Fusion Middleware Enterprise Deployment Guide for Exalogic*.
- **Storage Details**: In this section you enter the name used to access the ZFS storage device. This is the name that will be used in the **Storage** tab referenced as `appliance_name`.
- **Storage Shares**: In this section you enter the details of the ZFS Projects and Shares that you have (or need to) create on the ZFS Appliance. Example Project and Share Names have been provided. Complete the worksheet with the actual share names you have created. When you create a share on the ZFS appliance it will be assigned an Export Name usually in the following format:

  `/export/project_name/share_name`

  Enter this value in the **Export Name** column. The Export Name, in conjunction with the storage Name, can be used to complete the share name in the **Storage** tab.

  Note the following additional columns in this table:

  – **Mount Point**: The mount point is the name of the directory as mounted on the host, this is the same as the mount point on the **Storage** Tab.

  – **Mounted On Hosts**: This shows the hosts that the share should be mounted on. This information will be populated with values entered in the **Hardware** tab.

  For complete information on creating Exalogic Shares refer to the Storage Section of the *Oracle Fusion Middleware Enterprise Deployment Guide for Exalogic*.
- **Virtual Host Details**: This section lists the virtual hosts required by the typical enterprise deployment. Complete this section as follows:

  – **Network** - Select the Exalogic Network Type you wish to use for communication with the WebLogic managed servers, this is either IPoIB or EoIB.

  – **Actual Virtual Host Name** - Specify the host name associated with the network you wish to use for communication.

  – **IP Address** - Although not necessary for the deployment, it is worth making a note of the IP address associated with the **Actual Virtual Host Name**. This is

particularly useful where IPoIB networks are being used and host name resolution occurs using the local `/etc/hosts` file rather than the DNS.

- **OTD Failover Groups:** When you are deploying the software on Exalogic, this table lists the Oracle Traffic Director abstract virtual host names, and provides files where you can enter the actual host names and IP addresses that are defined for the OTD failover groups.

5

Procuring Resources for an Enterprise Deployment

Use this chapter to procure the required hardware, software, and network settings before you begin configuring the Oracle Identity and Access Management reference topology.

This chapter contains the following sections:

- Hardware and Software Requirements for an Enterprise Deployment
- Exalogic Requirements for an Enterprise Deployment
- Reserving the Required IP Addresses for an Enterprise Deployment
- Identifying and Obtaining Software Downloads for an Enterprise Deployment

5.1 Hardware and Software Requirements for an Enterprise Deployment

This section includes the following sections:

- Section 5.1.1, "Hardware Load Balancer Requirements"
- Section 5.1.2, "Host Computer Hardware Requirements"
- Section 5.1.3, "Operating System Requirements for the Enterprise Deployment Topology"

5.1.1 Hardware Load Balancer Requirements

This enterprise topology uses an external load balancer. This external load balancer should 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 should be possible so that incoming requests on the virtual host name and port are directed to a different port on the backend servers.
- Monitoring of ports on the servers in the pool to determine availability of a service.
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:

  - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle HTTP Server in the web tier, the load balancer needs to 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.
- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend 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. Examples of this include cookie-based persistence, IP-based persistence, and so on.
- The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the backend real servers using the equivalent non-SSL protocol (for example, HTTPS to HTTP).
- SSL acceleration (this feature is recommended, but not required for the enterprise topology).

5.1.2 Host Computer Hardware Requirements

The following sections provide information to help you procure host computers that are configured to support the Oracle Identity and Access Management enterprise deployment topologies:

- Section 5.1.2.1, "General Considerations for Enterprise Deployment Host Computers"
- Section 5.1.2.2, "Reviewing the Oracle Fusion Middleware System Requirements"
- Section 5.1.2.3, "Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment"
- Section 5.1.2.4, "Typical Disk Space Requirements for an Oracle Identity and Access Management"

5.1.2.1 General Considerations for Enterprise Deployment Host Computers

Before you start the process of configuring an Oracle Fusion Middleware enterprise deployment, you must perform the appropriate capacity planning to determine the number of nodes, CPU, and memory requirements for each node depending on the specific system's load as well as the throughput and response requirements. These requirements will vary for each application or custom IAM system being used.

The information in this chapter provides general guidelines and information that will help you determine the host computer requirements. It does not replace the need to perform capacity planning for your specific production environment.

Workbook Note: As you obtain and reserve the host computers in this section, note the host names and system characteristics in the Enterprise Deployment Workbook. You will use these addresses later when you enable the IP addresses on each host computer.

For more information, see Chapter 4, "Using the Enterprise Deployment Workbook."

5.1.2.2 Reviewing the Oracle Fusion Middleware System Requirements

Review the *Oracle Fusion Middleware System Requirements and Specifications* to ensure that your environment meets the minimum installation requirements for the products you are installing.

The Requirements and Specifications document contains information about general Oracle Fusion Middleware hardware and software requirements, minimum disk space and memory requirements, database schema requirements, and required operating system libraries and packages.

It also provides some general guidelines for estimating the memory requirements for your Oracle Fusion Middleware deployment.

5.1.2.3 Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment

Table 5–1 summarizes the memory, file descriptors, and processes required for the Administration Server and each of the Managed Servers computers in a typical Oracle Identity and Access Management enterprise deployment. These values are provided as an example only, but they can be used to estimate the minimum amount of memory required for an initial enterprise deployment.

The example in Table 5–1 reflects the minimum requirements for configuring the Managed Servers and other services required on IAMHOST1, as depicted in the reference topologies in Section 2.1, "Understanding the Primary and Build-Your-Own Enterprise Deployment Topologies".

When you are procuring machines, use the information in the **Approximate Top Memory** column as a guide when determining how much physical memory each host computer should have available.

After you procure the host computer hardware and verify the operating system requirements, review the software configuration to be sure the operating system settings are configured to accommodate the number of open files listed in the **File Descriptors** column and the number processes listed in the **Operating System Processes and Tasks** column.

Table 5–1 Typical Memory, File Descriptors, and Processes Required for Each Enterprise Deployment Host

Managed Server, Utility, or Service	Approximate Top Memory	Number of File Descriptors	Operating System Processes and Tasks
Access Administration Server	3.0 GB	1300	180
Governance Administration Server	3.0 GB	2100	100
WLS_SOA	2.0 GB	1400	210
WLS_OIM	2.0 GB	1400	190

Table 5–1 (Cont.) Typical Memory, File Descriptors, and Processes Required for Each Enterprise Deployment Host

Managed Server, Utility, or Service	Approximate Top Memory	Number of File Descriptors	Operating System Processes and Tasks
WLS_BI	2.0 GB	900	100
WLS_OAM	1.0 GB	900	170
WLS_AMA	2.0 GB	1200	160
WLS_MSM	2.0 GB	900	120
Node Manager	268 MB	300	20

5.1.2.4 Typical Disk Space Requirements for an Oracle Identity and Access Management

For the latest disk space requirements for the Oracle Fusion Middleware 11*g* (11.1.2.3) products, including the Oracle Identity and Access Management products, review the *Oracle Fusion Middleware System Requirements and Specifications*.

Use the this information and the information in Section 7, "Preparing Storage for an Enterprise Deployment" to determine the disk space requirements required for your deployment.

Table 5–2 Typical Disk Space Requirements for a Oracle Identity and Access Management Enterprise Deployment

Server	Local Storage Required (per host)	Shared Storage Required
Oracle Web Tier	5 GB	
Oracle Directory	5 GB	10 GB
Oracle Access Manager	3 GB	10 GB
Oracle Governance	3 GB	10 GB
Life Cycle Management tools including software repository		30 GB

5.1.3 Operating System Requirements for the Enterprise Deployment Topology

The Oracle Fusion Middleware software products and components described in this guide are certified on various operating systems and platforms, which are listed in the *Oracle Fusion Middleware Supported System Configurations*.

About the Examples in this Guide: This guide focuses on the implementation of the enterprise deployment reference topology on Oracle Linux systems.

The topology can be implemented on any certified, supported operating system, but the examples in this guide typically show the commands and configuration steps as they should be performed using the bash shell on Oracle Linux.

5.2 Exalogic Requirements for an Enterprise Deployment

This section describes Exalogic requirements for an enterprise deployment.

This section contains the following topics:

- Section 5.2.1, "Exalogic Virtual Server Requirements"
- Section 5.2.2, "About Private Networks"
- Section 5.2.3, "About Exalogic Elastic Cloud Networks"
- Section 5.2.4, "About Virtual Server Templates"

5.2.1 Exalogic Virtual Server Requirements

If you are deploying onto an Exalogic Virtual deployment then you will need to create the following virtual servers in order to be able to host a typical Oracle Identity and Access Management Enterprise Deployment.

- Section 5.2.1.1, "Virtual Servers Required for IAM on Exalogic"
- Section 5.2.1.2, "About Distribution Groups"

> **Note:** As you obtain and reserve the host computers in this section, note the host names and system characteristics in the Enterprise Deployment Workbook. Use these addresses later when you enable the IP addresses on each host computer. For more information, see Chapter 4, "Using the Enterprise Deployment Workbook."

5.2.1.1 Virtual Servers Required for IAM on Exalogic

When you deploy the Oracle Identity and Access Management software as part of a virtual configuration on an Exalogic system, then you must be sure to configure the vServers shown in Table 5–3.

Table 5–3 vServer Information

Name	vServerType	Virtual Networks	Host Name	Distribution Group
otdhost1	LARGE	IPoIB-EDG[1]	otdhost1	IAM_OTD
		EoIB-client[2]	otdhost1-ext	
		IPoIB-Storage[3]	otdhost1-stor	
otdhost2	LARGE	IPoIB-EDG	otdhost2	IAM_OTD
		EoIB-client	otdhost2-ext	
		IPoIB-Storage	otdhost2-stor	
oamhost1	EXTRA_LARGE	IPoIB-EDG	oamhost1	IAM_IAD
		EoIB-client	oamhost1-ext	
		IPoIB-Storage	oamhost1-stor	
oamhost2	EXTRA_LARGE	IPoIB-EDG	oamhost2	IAM_IAD
		EoIB-client	oamhost2-ext	
		IPoIB-Storage	oamhost2-stor	
oimhost1	EXTRA_LARGE	IPoIB-EDG	oimhost1	IAM_IAG
		EoIB-client	oimhost1-ext	
		IPoIB-Storage	oimhost1-stor	

Table 5–3 (Cont.) vServer Information

Name	vServerType	Virtual Networks	Host Name	Distribution Group
oimhost2	EXTRA_LARGE	IPoIB-EDG	oimhost2	IAM_IAG
		EoIB-client	oimhost2-ext	
		IPoIB-Storage	oimhost2-stor	
ldaphost1	EXTRA_LARGE	IPoIB-EDG	ldaphost1	IAM_LDAP
		IPoIB-Storage	ldaphost1-stor	
ldaphost2	EXTRA_LARGE	IPoIB-EDG	ldaphost2	IAM_LDAP
		IPoIB-Storage	ldaphost2-stor	

[1] IPoIB-EDG is the internal IPoIB network used for inter vServer communication

[2] EoIB-client is the Client Access Network which connects to the corporate ethernet

[3] IPoIB-Storage is the internal network that vServers use to communicate with the ZFS storage appliance.

5.2.1.2 About Distribution Groups

Distribution groups are used to ensure that the same application running in multiple virtual servers do not all run on the same physical host. By preventing different vServers of the same type running on the same physical server, you prevent the failure of the underlying physical server from taking out the complete system.

For an Oracle Fusion Middleware Enterprise Deployment you need to the following Distribution Groups:

- EDG_OTD: Prevents two Oracle Traffic Director Servers from running on the same physical server
- EDG_OAM: Prevents two IAMAccessDomain Servers from running on the same physical server
- EDG_OIM: Prevents two IAMGovernanceDomain Servers from running on the same physical server
- EDG_LDAP: Prevents two LDAP servers running on the same physical server.

5.2.2 About Private Networks

If you are going to keep interapp communication on the internal network. Then you must create a private VLAN. In virtual Exalogic this is done via EMOC, in physical Exalogic this is done manually. When creating a private network in EMOC for IAM, you must allow space for at least 20 IP addresses. Instructions for doing this are in the Exalogic Hardware Enterprise Deployment Guide.

5.2.3 About Exalogic Elastic Cloud Networks

When you commission Exalogic Elastic cloud a number of networks will be available for attachment to your virtual servers. The names may differ depending on how they were created at commissioning but the networks you will need are:

- EoIB-Client - This is the network used to connect to the main corporate network. Often known as the external network.
- IPoIB-EDG - This is the private network used for inter app communication. The outside world cannot connect to it.
- IPoIB-Storage - This is the private network that virtual servers use to connect to the ZFS storage appliance.

5.2.4 About Virtual Server Templates

When you commission the Oracle Exalogic Elastic Cloud, a number of virtual server templates will be used.

The following are the typical virtual server templates that are created in Oracle Exalogic Elastic Cloud. You can customize these values depending on the results of your capacity planning.

Table 5–4 Virtual Server Templates

Type	Description	Memory (GB)	Number of Virtual CPUs
VERY_LARGE	Large Memory Intensive Applications	20	6
EXTRA_ LARGE	CPU Intensive Applications	16	6
LARGE	Average Intensity Applications	8	2
SMALL	Low intensity applications	4	1

5.3 Reserving the Required IP Addresses for an Enterprise Deployment

Before you begin installing and configuring the enterprise topology, you must obtain and reserve a set of IP addresses:

- Physical IP (IP) addresses for each of the host computers you have procured for the topology
- Virtual IP (VIP) addresses for each Managed Server in the Oracle WebLogic Server domain
- A unique virtual host name to be mapped to each VIP.

You can then work with your network administrator to be sure these required VIPs are defined in your DNS server. (Alternatively, for non-production environments, you can use the /etc/hosts file to define these virtual hosts).

For more information, see the following sections:

- Section 5.3.1, "What Is a Virtual IP (VIP) Address?"
- Section 5.3.2, "Why Use Virtual Host Names and Virtual IP Addresses?"
- Section 5.3.3, "Physical and Virtual IP Addresses Required by the Enterprise Topology"

5.3.1 What Is a Virtual IP (VIP) Address?

A virtual IP address is an unused IP Address which belongs to the same subnet as the host's primary IP address. It is assigned to a host manually. Individual Managed Servers and Administration Servers within the Oracle WebLogic Server domain are configured to listen on this IP Address.

5.3.2 Why Use Virtual Host Names and Virtual IP Addresses?

For an enterprise deployment, in particular, it is important that a set of VIPs--and the virtual host names to which they are mapped--are reserved and enabled on the corporate network.

Alternatively hostnames can be resolved through appropriate `/etc/hosts` file propagated through the different nodes.

In the event of the failure of the host computer where the IP address is assigned, the IP address can be assigned to another host in the same subnet, so that the new host can take responsibility for running the managed servers assigned to it.

The reassignment of virtual IP addresses for Managed Servers can be performed automatically using the Server Migration feature of Oracle WebLogic Server. The reassignment of virtual IP address for the Administration Server must be performed manually.

Instructions for configuring Server Migration and for manually reassigning the Administration Server VIP are provided in Chapter 21, "Configuring Server Migration for an Enterprise Deployment."

5.3.3 Physical and Virtual IP Addresses Required by the Enterprise Topology

A virtual IP address is an unused IP Address which belongs to the same subnet as the host's primary IP address. It is assigned to a host manually and Oracle WebLogic Servers are configured to listen on this IP Address. In the event of the failure of the node where the IP address is assigned, the IP address is reassigned to another node in the same subnet, so that the new node can take responsibility for running the WebLogic Servers assigned to it. In other words, these virtual IP addresses are associated with a virtual host name. That way, should it be required, the underlying IP address can be changed.

The examples below show the virtual host names required by this document. These are associated with a virtual IP address as described above.

The following is a list of the virtual servers required by Oracle Identity and Access Management:

- IADADMINVHN.example.com

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

- IGDADMINVHN.example.com

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

- OIMHOSTxVHNn.example.com

  Where x is the host name and n is a unique number for the virtual host.

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

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

Configure the Administration Server and the managed servers to listen on different virtual IPs and physical IPs as illustrated in Figure 5–1.

You can assign any unique host name to the VIPs, but in this guide, we reference each VIP using the suggested host names in the table.

Workbook Note: As you obtain and reserve the IP addresses and their corresponding virtual host names in this section, note the values of the IP addresses and host names in the Enterprise Deployment Workbook. You will use these addresses later when you enable the IP addresses on each host computer.

For more information, see Chapter 4, "Using the Enterprise Deployment Workbook"

Figure 5–1 IP and VIrtual IP Addresses of the Servers in IAMAccessDomain

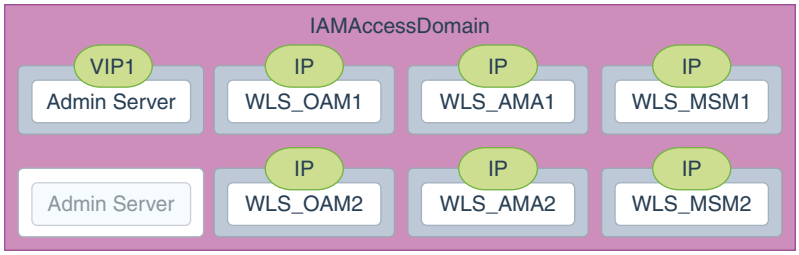


Figure 5–2 IP and Virtual IP Addresses of the Servers in IAMGovernanceDomain

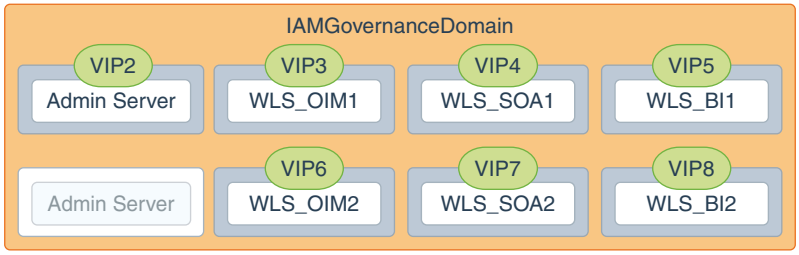


Table 5–5 Summary of the Virtual IP Addresses Required for the Oracle Identity and Access Management Enterprise Deployment Topology

Virtual IP	VIP Maps to...	Description
VIP1	IADADMINVHN	IADADMINVHN is the virtual host name used as the listen address for the Access Domain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running.
VIP2	IGDADMINVHN	IGDADMINVHN is the virtual host name used as the listen address for the Governance Domain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running.
VIP3	OIMHOST1VHN1	OIMHOST1VHN1 is the virtual host name that maps to the listen address for WLS_OIM1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_OIM1 process is running.
VIP4	OIMHOST1VHN2	OIMHOST1VHN2 is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_SOA1 process is running
VIP5	OIMHOST1VHN3	OIMHOST1VHN3 is the virtual host name that maps to the listen address for WLS_BI1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_BI1 process is running
VIP6	OIMHOST2VHN1	OIMHOST2VHN1 is the virtual host name that maps to the listen address for WLS_OIM2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_OIM2 process is running
VIP7	OIMHOST2VHN2	OIMHOST2VHN2 is the virtual host name that maps to the listen address for WLS_SOA2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_SOA2 process is running
VIP8	OIMHOST2VHN3	OIMHOST3VHN3 is the virtual host name that maps to the listen address for WLS_BI2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_BI2 process is running

5.4 Identifying and Obtaining Software Downloads for an Enterprise Deployment

The procedure for obtaining the Oracle Identity and Access Management software varies, depending on whether you are using the manual installation and configuration procedures or the Oracle Identity and Access Management Life Cycle Management (LCM) Tools for an automated installation and configuration:

- Section 5.4.1, "Obtaining the LCM Tools and Oracle Identity and Access Management Software Repository for an Automated Deployment"
- Section 5.4.2, "Obtaining Required Patches for an Automated Deployment with the LCM Tools"
- Section 5.4.3, "Applying Patches Automatically as Part of the LCM Tools Automated Deployment Process"
- Section 5.4.4, "Obtaining the Oracle Identity and Access Management Software for a Manual Deployment"
- Section 5.4.5, "Obtaining Patches for a Manual Deployment"

5.4.1 Obtaining the LCM Tools and Oracle Identity and Access Management Software Repository for an Automated Deployment

Before you can use the LCM Tools to automate the deployment of Oracle Identity and Access Management, you must locate and download the **Oracle Identity and Access Management Deployment Repository 11.1.2.3.0**.

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

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

For more information about the directory structure of the Oracle Identity and Access Management Deployment Repository, see Section 7.5.2, "About the Lifecycle Repository" and Section 7.5.5.1, "Life Cycle Management and Deployment Repository".

> **Note:** If you plan to deploy Oracle Identity and Access Management on Exalogic, then you must also download Oracle Traffic Director 11.1.1.9.0 and WebGate for Oracle Traffic Director 11.1.1.9.0 separately.

5.4.2 Obtaining Required Patches for an Automated Deployment with the LCM Tools

If you are using the LCM Tools to perform an automated deployment, then after you download the LCM Tools, you must download the latest LCM Tools bundle patch before attempting an automated deployment.

At the time this document was published, the latest available bundle patch was IDMLCM BUNDLE PATCH 11.1.2.3.160419, which is available at the following URL:

`https://updates.oracle.com/download/22083030.html`

Be sure to review the readme.html file that is packaged with in the downloadable patch archive. The readme.html file includes important information about installing the bundle patch, as well as information about additional installation requirements.

For more information about required patches, see the *Release Notes for Identity and Access Management*.

5.4.3 Applying Patches Automatically as Part of the LCM Tools Automated Deployment Process

If you are using Life Cycle Management tools to perform an automated deployment, patches can be applied at the time of commissioning. To do this, patches need to be downloaded and placed into specific locations within the software repository.

Before starting the deployment, download any patches that are listed in the Release Notes, plus any other patches that are appropriate for your environment. The deployment tool can apply these patches automatically at the time it runs.

Download the patches from `http://support.oracle.com` and expand each patch to the directory appropriate for the product, as listed in Table 5–6. If the directory does not exist, create it.

After expanding the patch, make sure that the Patch Directory (as listed in Table 5–6) contains a directory which is a number. That directory contains directories and files similar to:

- etc
- files
- README.txt

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

bundle_patch_no/product/product_patch_no

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

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

Table 5–6 Product Patch Directories in the Life Cycle Repository

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

5.4.4 Obtaining the Oracle Identity and Access Management Software for a Manual Deployment

For a manual enterprise deployment of Oracle Identity and Access Management, you must obtain all the software downloads listed in Table 5–7.

For information on obtaining Oracle Fusion Middleware 11*g* software, see the *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

Table 5–7 Oracle Software Required for an Oracle Identity and Access Management Enterprise Deployment

Product	Version
Oracle HTTP Server	11.1.1.9.0
Java	1.7
Oracle WebLogic Server	10.3.6.0
Oracle Identity and Access Management	11.1.2.3.0
Oracle Unified Directory	11.1.2.3.0
Oracle Internet Directory	11.1.1.9.0
Oracle Traffic Director	11.1.1.9.0
Oracle SOA Suite	11.1.1.9.0

Table 5–7 (Cont.) Oracle Software Required for an Oracle Identity and Access Management Enterprise Deployment

Product	Version
Oracle WebGate for Oracle HTTP Server	11.1.1.9.0
Oracle WebGate for Oracle Traffic Director	11.1.1.9.0
Repository Creation Utility	11.1.1.9.0

Note: You can also use the software repository described in Section 5.4.3, "Applying Patches Automatically as Part of the LCM Tools Automated Deployment Process".

5.4.5 Obtaining Patches for a Manual Deployment

Before using the manual procedures for installing and configuring an enterprise deployment, be sure you have obtained the latest patches from My Oracle Support. For more information, see the *Release Notes for Oracle Identity and Access Management*.

6

Preparing the Load Balancer and Firewalls for an Enterprise Deployment

This chapter describes the how to prepare your load balancer and firewalls for an enterprise deployment.

This chapter contains the following topics:

- Configuring Virtual Hosts on the Hardware Load Balancer
- Configuring Firewalls and Ports for an Oracle Identity and Access Management Deployment
- Configuring the Firewalls and Ports for an Exalogic Enterprise Deployment

6.1 Configuring Virtual Hosts on the Hardware Load Balancer

This section describes how to configure virtual hosts on the hardware load balancer.

This section contains the following topics:

- Section 6.1.1, "Overview of the Hardware Load Balancer"
- Section 6.1.2, "Typical Procedure for Configuring the Hardware Load Balancer"'
- Section 6.1.3, "Load Balancer Health Monitoring"
- Section 6.1.4, "Summary of the Virtual Servers Required for an Oracle Identity and Access Management Deployment"
- Section 6.1.5, "Summary of the Virtual Servers Required for an Oracle Identity and Access Management Exalogic Deployment"

6.1.1 Overview of the Hardware Load Balancer

As shown in the topology diagrams, you must configure the hardware load balancer to recognize and route requests to several virtual servers and associated ports for different types of network traffic and monitoring.

In the context of a load balancing device, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. It is typically represented by an IP address and a service, and it is used to distribute incoming client requests to the servers in the server pool.

The virtual servers should be configured to direct traffic to the appropriate host computers and ports for the various services available in the enterprise deployment.

6.1.2 Typical Procedure for Configuring the Hardware Load Balancer

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

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

6.1.3 Load Balancer Health Monitoring

The load balancer must be configured to check that the services in the Load Balancer Pool are available. Failure to do so will result in requests being sent to hosts where the service is not running.

Table 6–1 shows examples of how to determine whether a service is available:

Table 6–1 Examples Showing How to Determine Whether a Service is Available

Service	Monitor Type	Monitor Mechanism
OID	ldap	ldapbind to cn=orcladmin
OUD	ldap	ldapbind to cn=oudadmin
OHS	http	check for GET /\r\n
OTD	http	check for GET /\r\n
MSAS	https	check for GET /bmax/bmax.pac\r\n

6.1.4 Summary of the Virtual Servers Required for an Oracle Identity and Access Management Deployment

For an Oracle Identity and Access Management deployment on commodity hardware, configure your hardware load balancer as shown in Table 6–2.

Table 6–2 Load Balancer Configuration Details

Load Balancer Virtual Server	Server Pool	Protocol	SSL Termination	Other Required Configuration/Comments
login.example.com:443	webhost1.example.com:7777 webhost2.example.com:7777	HTTPS	Yes	Identity Management requires that the following be added to the HTTP header: Header Name: IS_SSL Header Value: ssl Header Name: WL-Proxy-SSL Header Value: true
prov.example.com:443	webhost1.example.com:7777 webhost2.example.com:7777	HTTPS		Identity Management requires that the following be added to the HTTP header: Header Name: IS_SSL Header Value: ssl Header Name: WL-Proxy-SSL Header Value: true
msas.example.com:9002	webhost1.example.com:9002 webhost2.example.com:9002	HTTPS	No	
iadadmin.example.com:80	webhost1.example.com:7777 webhost2.example.com:7777	HTTP		
igdadmin.example.com:80	webhost1.example.com:7777 webhost2.example.com:7777	HTTP		
iadinternal.example.com:7777	webhost1.example.com:7777 webhost2.example.com:7777			
igdinternal.example.com:7777	webhost1.example.com:7777 webhost2.example.com:7777			
idstore.example.com:1389	ldaphost1.example.com:1389 ldaphost2.example.com:1389			
idstore.example.com:1636	ldaphost1.example.com:1636 ldaphost2.example.com:1636			

Notes: Port 80 is the *HTTP_PORT* from the Worksheet

Port 443 is the *HTTPS_PORT* from the Worksheet

Port 7777 is the *OHS_PORT* from the Worksheet

Port 9002 is the *MSAS_PORT* from the Worksheet

Port 1389 is the *LDAP_PORT* from the Worksheet. The example given is for OUD.

Port 1636 is the *LDAP_SSL_PORT* from the worksheet. The example given is for OUD.

6.1.5 Summary of the Virtual Servers Required for an Oracle Identity and Access Management Exalogic Deployment

For an Oracle Identity and Access Management deployment on Exalogic hardware, configure your load balancer as shown in Table 6–3.

Table 6–3 Load Balancer Configuration Details

Load Balancer Virtual Server	Server Pool[1]	Server Pool (External OHS)	Protocol	SSL Termination	External	Other Required Configuration/Comments

`login.example.com:443`	`webhost1vhn1.example.com:7777`
	`webhost2vhn1.example.com:7777`
		`ohshost1.example.com:7777`
		`ohshost2.example.com:7777`
			HTTPS	Yes	Yes	Identity Management requires that the following be added to the HTTP header:
						`Header Name: IS_SSL`[2]
						`Header Value: ssl`
						`Header Name: WL-Proxy-SSL`
						`Header Value: true`

`prov.example.com:443`	`webhost1vhn1.example.com:7777`
	`webhost2vhn1.example.com:7777`
		`ohshost1.example.com:7777`
		`ohshost2.example.com:7777`
			HTTPS	Yes	Yes	Identity Management requires that the following be added to the HTTP header:
						`Header Name: IS_SSL`
						`Header Value: SSL`
						`Header Name: WL-Proxy-SSL`
						`Header Value: true`

`MSAS.example.com:9002`	`webhost1.example.com:9002` `webhost2.example.com:9002`	`ohshost1.example.com:9002` `ohshost2.example.com:9002`	HTTPS	No	Yes	This entry point passes through SSL rather than terminates it.

Table 6–3 (Cont.) Load Balancer Configuration Details

Load Balancer Virtual Server	Server Pool[1]	Server Pool (External OHS)	Protocol	SSL Termination	External	Other Required Configuration/Comments
IADADMIN.example.com:80	webhost1vhn1.example.com:7777 webhost2vhn1.example.com:7777	ohshost1.example.com:7777 ohshost2.example.com:7777	HTTP	No	No	
IGDADMIN.example.com:80	webhost1vhn1.example.com:7777 webhost2vhn1.example.com:7777	ohshost1.example.com:7777 ohshost2.example.com:7777	HTTP	No	No	

[1] If you do not want to use an OTD failover group for faster failover detection, substitute WEBHOST1-vhn and webhost2-vhn with the host names corresponding to the client access network. For example: iamhost1ext and iamhost2ext.

[2] For information about configuring IS_SSL, see "About User Defined WebGate Parameters" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

If you do not want to use an OTD failover group for faster failover detection, substitute WEBHOST1-VHN and WEBHOST2-VHN with the host names corresponding to the client access network. For example: WEBHOST1 and WEBHOST2.

In Exalogic deployments it is assumed that LDAP and inter app calls will be load balanced via OTD.

If you are using an external OHS then the servers will point to the external OHS hosts.

For information about configuring IS_SSL, see "About User Defined WebGate Parameters" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

Note: Port 80 is the *HTTP_PORT* from the Worksheet

Port 443 is the *HTTPS_PORT* from the Worksheet

Port *7777* is the *OHS_PORT* from the Worksheet

Port 9002 is the *MSAS_PORT* from the Worksheet

Port 1389 is the *LDAP_PORT* from the Worksheet

Port 1636 is the *LDAP_SSL_PORT* from the worksheet

6.2 Configuring Firewalls and Ports for an Oracle Identity and Access Management Deployment

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

Most port numbers are assigned after installation. You can use different port numbers if you want to. The port numbers shown in Table 6–4 are examples that are used throughout this guide for consistency. If you use different port numbers, you must substitute those values for the values in the table wherever they are used.

Table 6–4 lists the ports used in the Oracle Identity and Access Management topology, including the ports that you must open on the firewalls in the topology.

Firewall notation:

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

Table 6–4 Ports Used in the Oracle Identity and Access Management Enterprise Deployment Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Browser request	FW0	80	HTTP / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity and Access Management.
Browser request	FW0	443	HTTPS / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity and Access Management.
Browser request	FW1	80	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IAM.
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IAM.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 6.1, "Configuring Virtual Hosts on the Hardware Load Balancer."
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
Webtier Access to Oracle Weblogic Administration Server (IAMAccessDomain)	FW1	7001	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Webtier Access to Oracle Weblogic Administration Server (IAMGovernanceDomain)	FW1	7101	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Enterprise Manager Agent - web tier to Enterprise Manager	FW1	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
Oracle HTTP Server to WLS_OAM	FW1	14100	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the `mod_weblogic` parameters used.
Oracle HTTP Server WLS_OIM	FW1	14000	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the `mod_weblogic` parameters used
Oracle HTTP Server WLS_SOA	FW1	8001	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the `mod_weblogic` parameters used

Table 6–4 (Cont.) Ports Used in the Oracle Identity and Access Management Enterprise Deployment

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Oracle HTTP Server WLS_MSM	FW1	14180	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the `mod_weblogic` parameters used
Oracle HTTP Server WLS_AMA	FW1	14150	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the `mod_weblogic` parameters used
Oracle HTTP Server WLS_BI	FW1	9704	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the `mod_weblogic` parameters used
Oracle HTTP Server management by Administration Server	FW1	OPMN remote port (6701) and OHS Administration Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period, such as 5-10 seconds.
Access Manager Server	FW1	5575	OAP	Both	N/A
Access Manager Coherence port	FW1	9095	TCMP	Both	N/A
Oracle Coherence Port	FW1	8000 - 8088	TCMP	Both	N/A
Application Tier to Database Listener	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Identity and Access Management.
Oracle Notification Server (ONS)	FW2	6200	ONS	Both	Required for Gridlink. An ONS server runs on each database server.
OUD Port	FW2	1389	LDAP	Inbound	Ideally, these connections should be configured not to time out.
OUD SSL Port	FW2	14636	LDAPS	Inbound	Ideally, these connections should be configured not to time out.
Load Balancer LDAP Port	FW2	386	LDAP	Inbound	Ideally, these connections should be configured not to time out.
Load Balancer LDAP SSL Port	FW2	636	LDAPS	Inbound	Ideally, these connections should be configured not to time out.
Node Manager	N/A	5556	TCP/IP	N/A	N/A
Oracle Unified Directory Replication	N/A	8989	TCP/IP	N/A	N/A

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

6.3 Configuring the Firewalls and Ports for an Exalogic Enterprise Deployment

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

Most port numbers are assigned during installation.

Table 6–5 lists the ports used in the Oracle Identity and Access Management topology, including the ports that you must open on the firewalls in the topology.

Note: In Table 6–5:

- 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 data tier

On Exalogic systems:

- FW1 is in between the load balancer and the Exadata Machine, unless an External OHS is used
- FW2 will be present only if your database does not reside on Exadata

---

Table 6–5 Ports Used in the Exalogic Reference Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
Load balancer to Oracle Traffic Director	FW0	7777	HTTP	n/a	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
Load Balancer to MSAS Proxy	FW0	9002	HTTP	n/a	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
IAMAccess Domain Administration Console access	FW1	7001	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).

Table 6–5 (Cont.) Ports Used in the Exalogic Reference Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
IAMGovernance Domain Administration Console access	FW1	7101	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Coherence	n/a	8088 Range: 8080 - 8090		n/a	n/a
Application tier to data tier (Oracle database or RAC outside of Oracle Exalogic machine via Ethernet)	FW2	1521		n/a	n/a
Oracle HTTP Server WLS_OAM	FW1	14100	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.
Oracle HTTP Server WLS_OIM	FW1	14000	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.
Oracle HTTP Server WLS_SOA	FW1	8001	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.

Table 6–5 (Cont.) Ports Used in the Exalogic Reference Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Oracle HTTP Server WLS_AMA	FW1	14150	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.
Oracle HTTP Server WLS_BI	FW1	9704	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.
Oracle HTTP Server WLS_MSM	FW1	14180	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.

7

Preparing Storage for an Enterprise Deployment

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

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

This chapter contains the following topics:

7.1 Overview of Preparing Storage for Enterprise Deployment

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

Use this chapter as a reference to help understand the directory variables used in the installation and configuration procedures. Other directory layouts are possible and supported, but the model adopted in this guide is chosen for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

7.2 Terminology for Directories and Directory Variables

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

- **IDM_TOP**: This environment variable and related directory path refers to the base directory under which the Oracle Binaries and configuration information is stored.

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

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

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

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

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

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

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

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

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

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

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

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

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

For more information about, and examples of these variables, see Section 7.5.5, "Recommended Directory Locations."

7.3 Overview of Enterprise Deployment Storage

When deciding how to prepare shared storage, consider the following:

Sharing Requirements

An artifact is either shared, or not-shared (or private), or available:

- Shared: The artifact resides on shared storage and can be simultaneously viewed and accessed by all client machines.

- Available: The artifact resides on shared storage, but only one client machine can view and access the artifact at a time. If this machine fails, another client machine can then access the artifact.
- Not-shared: The artifact can reside on local storage and never needs to be accessible by other machines.

Read/Write Requirements

An artifact will also have specific read/write requirements:

- Read-Only: This artifact is rarely altered but only read at runtime.
- Read-Write: This artifact is both read and written to at runtime.

Artifact Characteristics

With these requirements in mind, the artifacts deployed in a typical enterprise deployment are classified in Table 7–1.

Table 7–1 Typical Artifacts Deployed

Artifact type	Sharing	Read/Write
Binaries - Application Tier	Shared	Read-Only
Binaries - Web Tier	Private	Read-Only
Configuration - Directory Tier	Private	Read-Write
Configuration - Web Tier	Private	Read-Write
Managed Server Domain Home	Private	Read-Write
Admin Server Domain Home	Available	Read-Write
Runtime Files	Available	Read-Write
Node Manager Configuration	Private	Read-Write
Application Specific Files	Shared	Read-Write

7.4 About File Systems

After you create the partitions on your storage, you must place file systems on the partitions so that you can store the Oracle files. For local or direct attached shared storage, the file system type is most likely the default type for your operating system, for example: EXT3 for Linux.

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

7.5 Understanding the Enterprise Deployment Directory Structure

Each Oracle Fusion Middleware enterprise deployment is based on a similar directory structure. This directory structure has been designed to separate binaries, configuration, and runtime information. Binaries are defined as the Oracle software installation. Binaries include such things as the JDK, WebLogic Server, and the Oracle Fusion Middleware software being used (for example, Oracle Identity and Access Management or WebCenter).

The runtime directories are written to at runtime and hold information such as JMS queue files. The Server Domain Home directories are read from and written to at runtime.

For more information, see the following topics:

- Section 7.5.1, "Recommendations for Binary (Middleware Home) Directories"
- Section 7.5.2, "About the Lifecycle Repository"
- Section 7.5.3, "Recommendations for Domain Configuration Files"
- Section 7.5.4, "Shared Storage Recommendations for Runtime Files"
- Section 7.5.5, "Recommended Directory Locations"

7.5.1 Recommendations for Binary (Middleware Home) Directories

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

- Section 7.5.1.1, "About the Binary (Middleware Home) Directories"
- Section 7.5.1.2, "About Sharing a Single Middleware Home"
- Section 7.5.1.3, "About Using Redundant Binary (Middleware Home) Directories"

7.5.1.1 About the Binary (Middleware Home) Directories

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

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

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

In a multi-tiered deployment, it is often not possible to mount a single share across the tiers. For example, the directory tier to the application tier. For LDAP deployments, you have three options:

- Create a separate share for the directory binaries which is mounted only to the LDAP hosts using the same mount point as that of the application tier binaries. For example: `/u01/oracle/products`

  This option is recommended if you have firewalls between your zones.

- Use the same share for both the application tier and the directory tier.

  This option is recommended if firewalls are not used between the directory and the application tiers. For example, in Exalogic deployments.

- Install the directory binaries locally.

  This option is only applicable if you are performing a manual deployment.

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

For more information about the structure and content of an Oracle Fusion Middleware home, see Section 7.2, "Terminology for Directories and Directory Variables".

7.5.1.2 About Sharing a Single Middleware Home

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

This enterprise deployment guide uses one middleware home per domain with additional middleware homes for directory and the Web servers.

The advantage of using multiple middleware homes is that they can be patched independently, placing no dependencies on common files. In this way it is possible to patch directory at a different time to identity, which may be patched at a different time to access.

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

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

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

7.5.1.3 About Using Redundant Binary (Middleware Home) Directories

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

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

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

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

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

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

7.5.2 About the Lifecycle Repository

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

It is recommended that the lifecycle repository be mounted onto every host in the topology for the duration of provisioning. This allows the deployment process to place files into this location ready for use by other process steps that might be running on different hosts. Having a centralized repository saves you from having to manually copy files around during the provisioning process.

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

The advantages of having a shared lifecycle repository are:

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

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

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

7.5.3 Recommendations for Domain Configuration Files

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

- Section 7.5.3.1, "About Oracle WebLogic Server Administration and Managed Server Domain Configuration Files"
- Section 7.5.3.2, "Shared Storage Requirements for Administration Server Domain Configuration Files"
- Section 7.5.3.3, "Local Storage Requirements for Managed Server Domain Configuration Files"

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

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

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

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

ASERVER_HOME is the primary location of the domain configuration. *MSERVER_HOME* is a copy of the domain configuration that is used to start and stop managed servers. The WebLogic Administration Server automatically copies configuration changes applied to the *ASERVER_HOME* domain configuration to all those *MSERVER_HOME* configuration directories that have been registered to be part of the domain. However, the *MSERVER_*

HOME directories also contain deployments and data specific to the managed servers. For that reason, when performing backups, you must include both *ASERVER_HOME* and *MSERVER_HOME*.

7.5.3.2 Shared Storage Requirements for Administration Server Domain Configuration Files

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

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

7.5.3.3 Local Storage Requirements for Managed Server Domain Configuration Files

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

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

7.5.4 Shared Storage Recommendations for Runtime Files

Files and directories that might need to be available to all members of a cluster are separated into their own directories. These include JMS files, transaction logs, and other artifacts that belong to only one member machine of a cluster, but might need to be available to other machines in case of failover.

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

Transaction logs' contents are relatively short-lived and their contents may usually relate to JMS operations. For backup and disaster protection purposes, it is important that both type of stores (jms and tlogs) are copied synchronously or continuously, and are in the same consistency group or replication_project as JMS stores (if multiple volumes are used for tlogs and jms replication). This way, immediate and synchronized copies of both stores are created. This will minimize data loss and will guaranty consistency.

7.5.5 Recommended Directory Locations

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

This section includes the following topics:

- Section 7.5.5.1, "Life Cycle Management and Deployment Repository"
- Section 7.5.5.2, "Shared Storage"
- Section 7.5.5.3, "Private Storage"

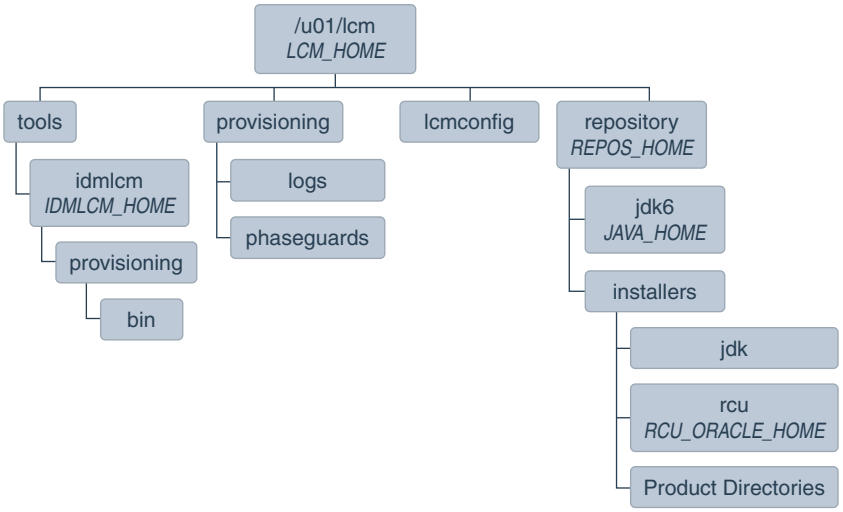
7.5.5.1 Life Cycle Management and Deployment Repository

A separate share is required to hold the Life Cycle Management tools and Deployment Repository. This share is only required during deployment and any subsequent patching. Once deployment is complete, you can unmount this share from each host.

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

Ideally, you should mount this share on ALL hosts for the duration of provisioning. Doing so will make the provisioning process simpler, as you will not need to manually copy any files, such as the keystores required by the Web Tier. If your organization prohibits sharing the LCM_HOME to the Web tier hosts (even for the duration of deployment), you must create a local copy of the contents of this share on the DMZ hosts and make manual file copies during the deployment phases.

Figure 7–1 Deployment Repository



> **Note:** The Life Cycle Management Repository is mandatory for LCM deployments. For Manual deployments, it is recommended. For simplicity, this guide assumes that you are using a deployment repository for both LCM and manual deployments.
>
> If you download the software repository from `http://edelivery.oracle.com`, then the repository directory tree will be created for you. If you download the products individually, then you need to create the directory tree and create a separate sub directory for each product.

7.5.5.2 Shared Storage

In an Enterprise Deployment for IAM the following shared storage is required. The shared storage you create is the same regardless of whether you are creating a consolidated or distributed deployment. What does differ is the hosts you mount that shared on.

The recommended layout is described in Table 7–2 and Table 7–3 and shown in Figure 7–2.

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

Table 7–2 Volumes on Shared Storage–Distributed Topology

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

[1] Only mount to LDAPHOST1 and LDAPHOST2 when directory is in the Application Zone
[2] Only required when directory is being placed into a Directory/Database Zone

Table 7–3 Volumes on Shared Storage–Consolidated Topology

Environment Variable	Volume Name	Mount Point	Mounted on Hosts	Exclusive
SW_ROOT	Binaries	/u01/oracle/products	IAMHOST1 IAMHOST2 LDAPHOST1 LDAPHOST2[1]	No
SHARED_ CONFIG_DIR	sharedConfig	/u01/oracle/config	IAMHOST1 IAMHOST2	No
RT_HOME	runTime	/u01/oracle/runtime	IAMHOST1 IAMHOST2	

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

Notes on Shared Storage

Oracle IAM requires shared storage for product binaries and for shared configuration information.

If you are using a dedicated directory zone, and your organization prohibits the mounting of storage across zones, create a separate binary share for the directory tier.

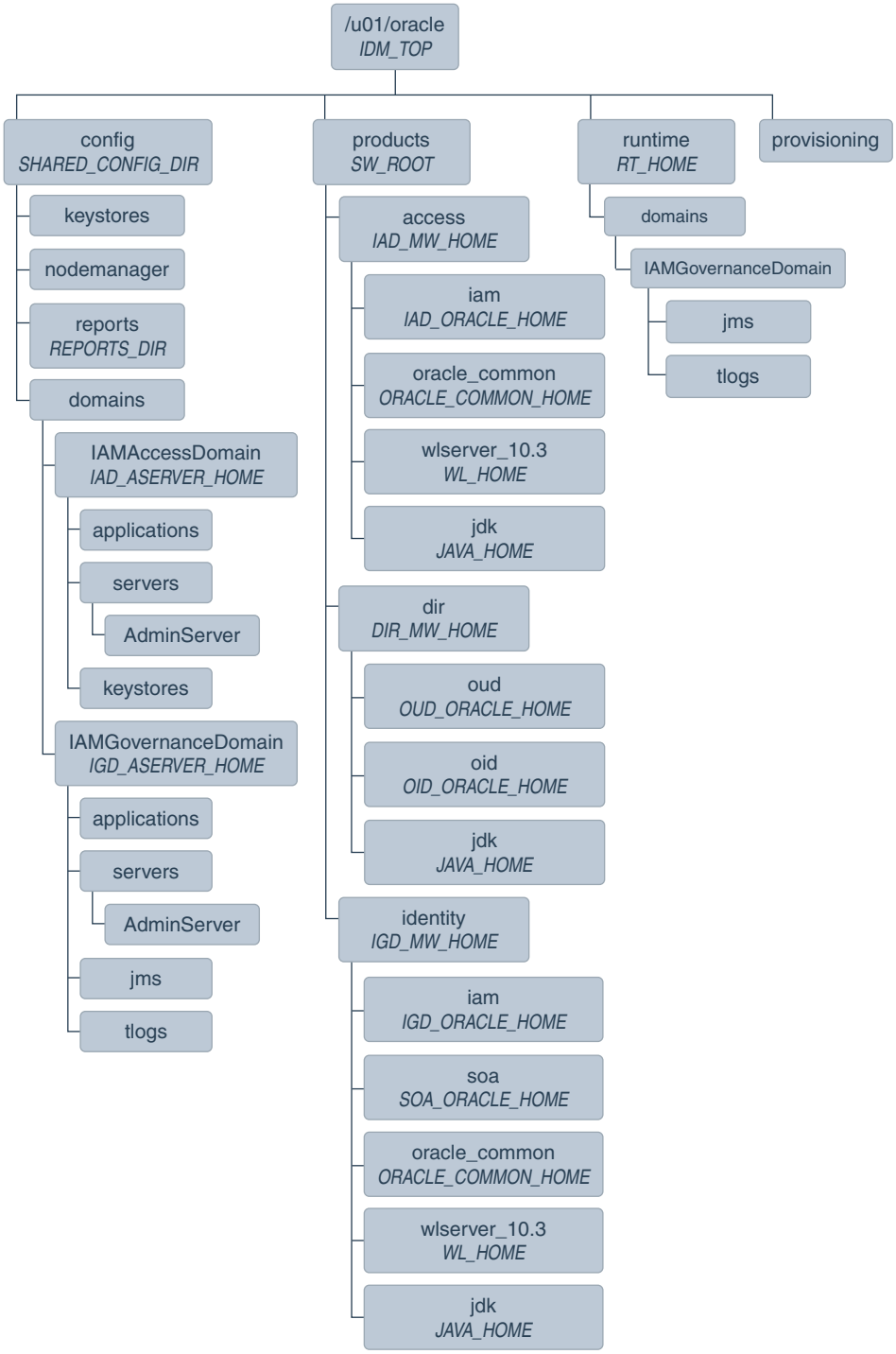
If, however, you are not creating a separate directory zone, or if you are not prevented from mounting file systems across zones, you require only one share for all binaries (except Web Tier binaries).

In an Exalogic deployment, it is not necessary to separate out the binaries for the directory and application tiers.

If you do create two different binary shares (one for the application tier and one for the directory tier), they must have the same host mount point.

If you are using NFSv4, you will need a NIS server. You must ensure that the users referenced in Section 9.7, "Configuring Users and Groups" are created in NIS server, prior to being able to grant storage ownership to those NIS users.

Figure 7–2 Recommended Shared Storage Directory Structure



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

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

The directory config contains domains, which contains:

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

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

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

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

The directory runtime is used to store artefacts generated at runtime. For example, JMS and TLOG files.

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

7.5.5.3 Private Storage

Private storage refers to shared disk volumes that have been exclusively mounted or local storage.

Every host uses private storage for configuration information. In addition, the Web Tier hosts can store their binaries on private storage. This is especially important where the Web Tier hosts reside in a DMZ.

If you are installing on physical Exalogic without an external OHS, it is recommended that WEB_MW_HOME be placed onto shared storage. This is because, the OTD host is inside the Exalogic appliance and therefore has access to the ZFS storage device.

If you are installing on virtual Exalogic, it is recommended that the exclusively mounted shares on the shared storage are used, to enable simpler backups.

If you are using Exalogic or are mounting NFS shares to your web tier, then Webtier binaries can also reside on shared storage. The mount point for the binaries is the same whether it is on shared or private storage. If you are using Exalogic physical deployment where the web tier and the application tier are on the same compute nodes, then you do not need to create a separate share for the webtier binaries.

Table 7–4 Private Storage Directories - Distributed Topology

Tier	Environment Variable	Directory	Hosts
Web Tier	*WEB_MW_HOME*	/u01/oracle/products	WEBHOST1 WEBHOST2

Table 7–4 (Cont.) Private Storage Directories - Distributed Topology

Tier	Environment Variable	Directory	Hosts
	OHS_ORACLE_INSTANCE	/u02/private/oracle/config/instances/ohs*n*	WEBHOST1 WEBHOST2
	OTD_ORACLE_INSTANCE	/u02/private/oracle/config/instances/otdn	WEBHOST1 WEBHOST2
	MSAS_ORACLE_INSTANCE	/u02/private/oracle/config/instances/gatewayid	WEBHOST1 WEBHOST2
	OTD_ORACLE_HOME	/u01/oracle/products/web/otd	WEBHOST1 WEBHOST2
	OHS_ORACLE_HOME	/u01/oracle/products/web/ohs	WEBHOST1 WEBHOST2
Application Tier	*LDAP_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oid*n*	LDAPHOST1 LDAPHOST2
	IAD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMAccessDomain	OAMHOST1 OAMHOST2
	IGD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMGovernanceDomain	OIMHOST1 OIMHOST2
Directory Tier	*DIR_MW_HOME*[1]	/u01/oracle/products	LDAPHOST1 LDAPHOST2
	OUD_ORACLE_INSTANCE	/u02/private/oracle/config/instances/oudn	LDAPHOST1 LDAPHOST2
	OID_ORACLE_INSTANCE	/u02/private/oracle/config/instances/oidn	LDAPHOST1 LDAPHOST2

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

Table 7–5 Private Storage Directories - Consolidated Topology

Tier	Environment Variable	Directory	Hosts
Web Tier	*WEB_MW_HOME*	/u01/oracle/products	WEBHOST1 WEBHOST2
	OHS_ORACLE_INSTANCE	/u02/private/oracle/config/instances/ohs*n*	WEBHOST1 WEBHOST2
	OTD_ORACLE_INSTANCE	/u02/private/oracle/config/instances/otdn	WEBHOST1 WEBHOST2
	MSAS_ORACLE_INSTANCE	/u02/private/oracle/config/instances/gatewayid	WEBHOST1 WEBHOST2
	OTD_ORACLE_HOME	/u01/oracle/products/web/otd	WEBHOST1 WEBHOST2

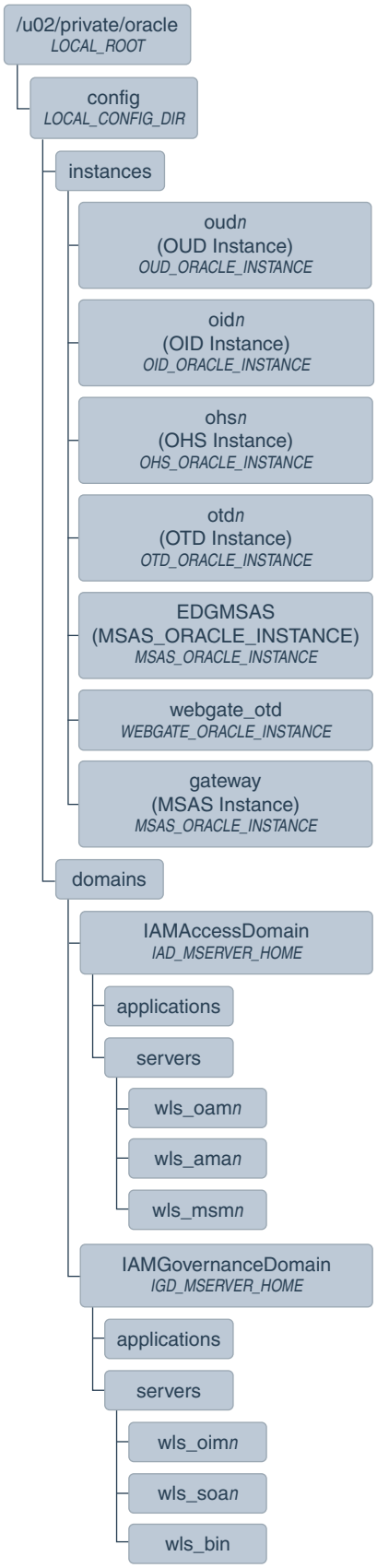
Table 7–5 (Cont.) Private Storage Directories - Consolidated Topology

Tier	Environment Variable	Directory	Hosts
	OHS_ORACLE_HOME	/u01/oracle/products/web/ohs	WEBHOST1 WEBHOST2
Application Tier	*LDAP_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oid*n*	IAMHOST1 IAMHOST2
	IAD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMAccessDomain	IAMHOST1 IAMHOST2
	IGD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMGovernanceDomain	IAMHOST1 IAMHOST2
Directory Tier	*DIR_MW_HOME*[1]	/u01/oracle/products	IAMHOST1 IAMHOST2
	OUD_ORACLE_INSTANCE	/u02/private/oracle/config/instances/oudn	IAMHOST1 IAMHOST2
	OID_ORACLE_INSTANCE	/u02/private/oracle/config/instances/oidn	IAMHOST1 IAMHOST2

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

Note: *OTD_ORACLE_HOME* is only used when Oracle Traffic Director is deployed.

Figure 7–3 Recommended Private Storage Directory Structure



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

Note: The otd*n* directory is only for Exalogic deployments.

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

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

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

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

Figure 7–4 Recommended Directory Structure for Private Binary Storage on Webhosts

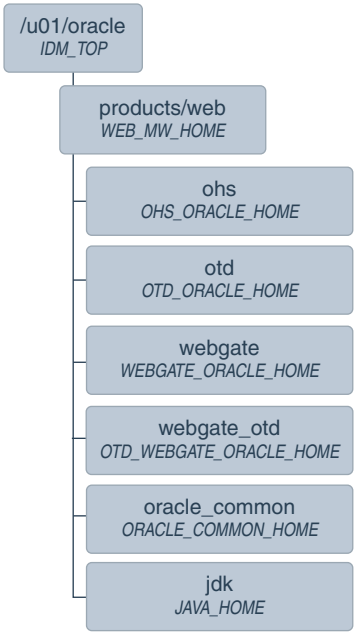


Figure 7–4 shows the local binary storage directory hierarchy. The top level directory, `/u01/oracle` (*IDM_TOP*), has a subdirectory, `products`.

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

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

8

Preparing Exalogic for an Oracle Identity and Access Management Deployment

Preparing Exalogic consists of performing all of the previous preparatory steps on an Exalogic appliance. Once completed, the environment will have the same structure as a traditional server deployment. The steps to prepare Exalogic are in the *Oracle Fusion Middleware Enterprise Deployment Guide for Exalogic*.

This section of the document, summarizes the previous sections from an Exalogic point of view.

This chapter contains the following sections:

8.1 Summary of Virtual IP Addresses Required

You need to allocate the following Virtual IP Addresses on Exalogic:

Table 8–1 Summary of the Virtual IP Addresses Required for the IAM Enterprise Deployment Topology

Virtual IP	Variable	Documented Value
VIP1	IADADMINVHN	IADADMINVHN is the virtual host name used as the listen address for the Access Domain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running
VIP2	IGDADMINVHN	IGDADMINVHN is the virtual host name used as the listen address for the Governance Domain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running
VIP3	OIMHOST1VHN1	OIMHOST1VHN1 is the virtual host name that maps to the listen address for WLS_OIM1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_OIM1 process is running
VIP4	OIMHOST1VHN2	OIMHOST1VHN2 is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_SOA1 process is running
VIP5	OIMHOST1VHN3	OIMHOST1VHN3 is the virtual host name that maps to the listen address for WLS_BI1 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_BI1 process is running

Table 8–1 (Cont.) Summary of the Virtual IP Addresses Required for the IAM Enterprise Deployment

Virtual IP	Variable	Documented Value
VIP6	OIMHOST2VHN1	OIMHOST2VHN1 is the virtual host name that maps to the listen address for WLS_OIM2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_OIM2 process is running
VIP7	OIMHOST2VHN2	OIMHOST2VHN2 is the virtual host name that maps to the listen address for WLS_SOA2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_SOA2 process is running
VIP8	OIMHOST2VHN3	OIMHOST2VHN3 is the virtual host name that maps to the listen address for WLS_BI2 and fails over with Whole Server Migration of this managed server. It is enabled on the node where WLS_BI2 process is running

8.2 Summary of Storage Requirements

This section summarizes storage requirements for an Oracle Identity and Access Management deployment on Exalogic.

- Section 8.2.1, "Summary of the Storage Appliance Directories and Corresponding Mount Points for Physical Exalogic"
- Section 8.2.2, "Summary of the Storage Appliance Directories and Corresponding Mount Points for Virtual Exalogic"

8.2.1 Summary of the Storage Appliance Directories and Corresponding Mount Points for Physical Exalogic

For the Oracle Identity Management enterprise topology, you install all software products on the Sun ZFS Storage 7320 appliance, which is a standard hardware storage appliance available with every Exalogic machine. No software is installed on the local storage available for each compute node.

To organize the enterprise deployment software on the appliance, you create a new project, called `IAM`. The shares (`/products` and `/config`) are created within this project on the appliance, so you can later mount the shares to each compute node.

To separate the product binaries from the files specific to each compute node, you create a separate share for each compute node. Sub-directories are for the host names are created under `config` and `products` directories. Each private directory is identified by the logical host name; for example, `IAMHOST1` and `IAMHOST2`.

Figure 8–2 shows the recommended physical directory structure on the Sun ZFS Storage 7320 appliance.

Table 8–4 shows how the shares on the appliance map to the mount points you will create on the vServers.

Figure 8–1 Physical Structure of the Shares on the Sun ZFS Storage Appliance for Physical Exalogic Deployments

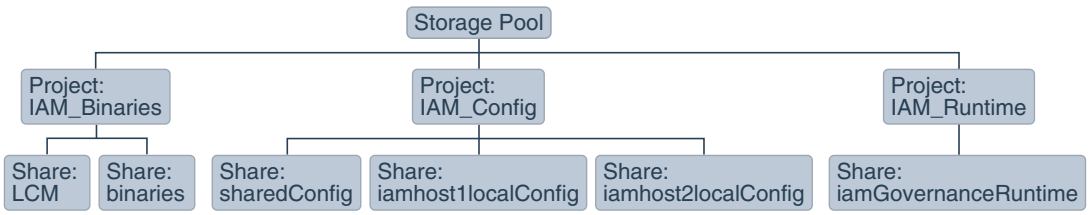


Figure 8–1 illustrates the physical structure of the shares on the Sun ZFS storage appliance

Table 8–2 Mapping the Shares on the Appliance to Mount Points on Each Compute Node

Project	Share	Mount Point	Host	Mounted On	Privileges to Assign to User, Group, and Other	Size
IAM_ Binaries	binaries	/export/IAM_ Binaries/bin aries	IAMHOST1 IAMHOST2	/u01/oracle/ products	R and W (Read and Write)	50 GB
IAM_ Binaries	LCM	/export/IAM_ Binaries/LCM	ALL Hosts	/u01/lcm	R and W (Read and Write)	50 GB
IAM_ Config	sharedCo nfig	/export/IAM_ Config/share dConfig	IAMHOST1 IAMHOST2	/u01/oracle/ config	R and W (Read and Write)	100 GB
IAM_ Config	iamhost1 localCon fig	/export/IAM_ Config/iamho st1localConf ig	IAMHOST1	/u02/private /oracle/conf ig	R and W (Read and Write)	100 GB
IAM_ Config	iamhost2 localCon fig	/export/IAM_ Config/iamho st2localConf ig	IAMHOST2	/u02/private /oracle/conf ig	R and W (Read and Write)	100 GB
IAM_ Runtime	iamGover nanceRun time	/export/IAM_ Runtime/iamG overnanceRun time	IAMHOST1 IAMHOST2	/u01/oracle/ runtime	R and W (Read and Write)	5 GB

Table 8–3 Summary of Storage Projects for Physical Exalogic

Project	Size
IAM_Binaries	100 GB
IAM_Config	300 GB
IAM_Runtime	5 GB

8.2.2 Summary of the Storage Appliance Directories and Corresponding Mount Points for Virtual Exalogic

For the Oracle Identity Management enterprise topology, you install all software products on the Sun ZFS Storage 7320 appliance, which is a standard hardware storage appliance available with every Exalogic machine. No software is installed on the local storage available for each compute node.

To organize the enterprise deployment software on the appliance, you create a new project, called `IAM`. The shares (`/products` and `/config`) are created within this project on the appliance, so you can later mount the shares to each compute node.

To separate the product binaries from the files specific to each compute node, you create a separate share for each compute node. Sub-directories are for the host names are created under `config` and `products` directories. Each private directory is identified by the logical host name; for example, `IAMHOST1` and `IAMHOST2`.

Figure 8–2 shows the recommended physical directory structure on the Sun ZFS Storage 7320 appliance.

Table 8–4 shows how the shares on the appliance map to the mount points you will create on the vServers that host the enterprise deployment software.

Figure 8–2 Physical Structure of the Shares on the Sun ZFS Storage Appliance for Virtual Exalogic Deployments

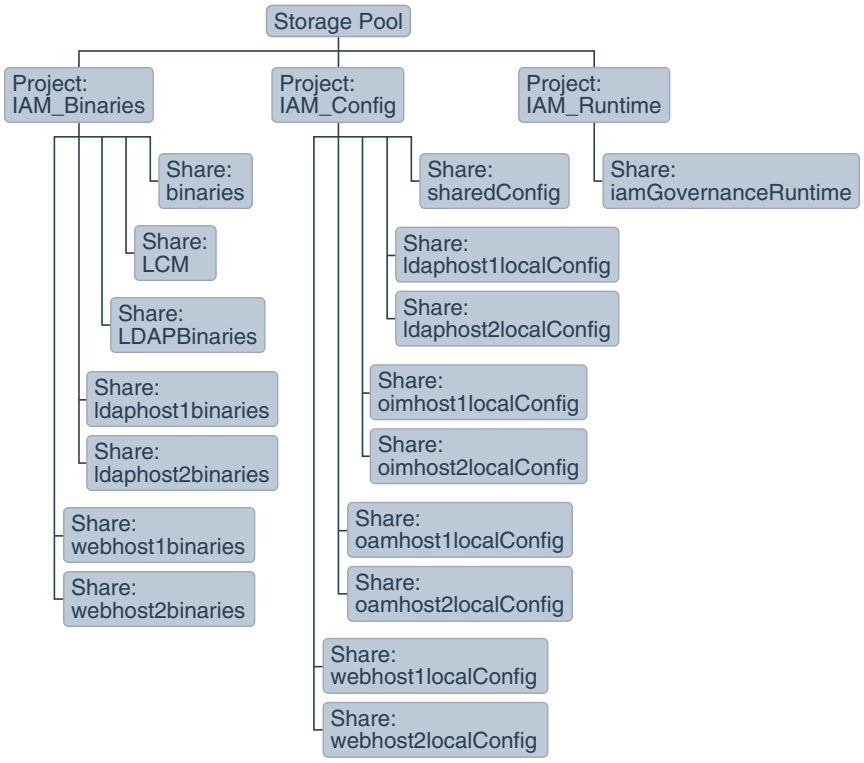


Figure 8–2 illustrates the physical structure of the shares on the Sun ZFS storage appliance.

Table 8–4 Mapping the Shares on the Appliance to Mount Points on Each vServer

Project	Share	Mount Point	Host	Mounted On	Privileges to Assign to User, Group, and Other	Actual Size
IAM_ Binaries	LCM	`/export/IAM_ Binaries/LCM`	ALL Hosts	`/u01/lcm`	R and W (Read and Write)	35 GB
IAM_ Binaries	`binaries`	`/export/IAM_ Binaries/binaries`	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	`/u01/oracle/products`	R and W (Read and Write)	35 GB
IAM_ Binaries	LDAPBinaries	`/export/IAM_ Binaries/LDAPBinaries`	LDAPHOST1 LDAPHOST2	`/u01/oracle/products`	R and W (Read and Write)	10 GB
IAM_ Binaries	`webhost1binaries`	`/export/IAM_ Binaries/webhost1binaries`	WEBHOST1	`/u01/oracle/products`	R and W (Read and Write)	10 GB

Table 8–4 (Cont.) Mapping the Shares on the Appliance to Mount Points on Each vServer

Project	Share	Mount Point	Host	Mounted On	Privileges to Assign to User, Group, and Other	Actual Size
IAM_ Binaries	webhost2binaries	/export/IAM_Binaries/webhost2binaries	WEBHOST2	/u01/oracle/products	R and W (Read and Write)	10 GB
IAM_ Config	sharedConfig	/export/IAM_Config/sharedConfig	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	/u01/oracle/config	R and W (Read and Write)	100 GB
IAM_ Config	oamhost1localConfig	/export/IAM_Config/oamhost1localConfig	OAMHOST1	/u02/private/oracle/config	R and W (Read and Write)	10 GB
IAM_ Config	oamhost2localConfig	/export/IAM_Config/oamhost2localConfig	OAMHOST2	/u02/private/oracle/config	R and W (Read and Write)	10 GB
IAM_ Config	oimhost1localConfig	/export/IAM_Config/oimhost1localConfig	OIMHOST1	/u02/private/oracle/config	R and W (Read and Write)	80 GB
IAM_ Config	oimhost2localConfig	/export/IAM_Config/oimhost2localConfig	OIMHOST2	/u02/private/oracle/config	R and W (Read and Write)	80 GB
IAM_ Config	webhost1localConfig	/export/IAM_Config/webhost1localConfig	WEBHOST1	/u02/private/oracle/config	R and W (Read and Write)	5 GB
IAM_ Config	webhost2localConfig	/export/IAM_Config/webhost2localConfig	WEBHOST2	/u02/private/oracle/config	R and W (Read and Write)	5 GB
IAM_ Config	ldaphost1localConfig	/export/IAM_Config/ldaphost1localConfig	LDAPHOST1	/u02/private/oracle/config	R and W (Read and Write)	5 GB
IAM_ Config	ldaphost2localConfig	/export/IAM_Config/ldaphost2localConfig	LDAPHOST2	/u02/private/oracle/config	R and W (Read and Write)	5 GB
IAM_ Runtime	iamGovernanceRuntime	/export/IAM_Runtime/iamGovernanceRuntime	OIMHOST1 OIMHOST2	/u01/oracle/runtime	R and W (Read and Write)	5 GB

Note: The `binary` directories can be changed to **read only** after the configuration is complete if desired. The LDAPHOST binaries have been split into two shares, one for each node. These can be combined, if required.

Table 8–5 Summary of Storage Projects for Virtual Exalogic

Project	Size
IAM_Binaries	100 GB
IAM_Config	300 GB
IAM_Runtime	5 GB

9

Configuring the Host Computers for an Enterprise Deployment

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

It contains the following sections:

9.1 Overview of Configuring the Hosts

Before you deploy Oracle Fusion Middleware, you must set up the hosts you plan to use so that the Oracle software can work in an optimum fashion.

The settings described in this chapter are only a guide. After using your Oracle software, you should use operating system utilities to tune the configuration to ensure that you are maximizing the potential of your hosts.

In the context of Exalogic, the hosts are either compute nodes in physical Exalogic or vServers in virtual Exalogic.

9.2 Verifying Your Host and Operating System

Ensure that the host and operating system that you plan to use is a certified combination for the products you plan to use. Refer to the Oracle Fusion Middleware Supported System Configurations for details.

9.3 Meeting the Minimum Hardware Requirements

In order to use a host in an enterprise deployment, you must verify that it meets the minimum specification described in Section 5.1, "Hardware and Software Requirements for an Enterprise Deployment".

In addition, you must check the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* to ensure that you have the minimum specification to support the products you plan to deploy on your hosts.

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

Ensure that you have sufficient local disk and that shared storage is configured as described in Chapter 7, "Preparing Storage for an Enterprise Deployment."

Allow sufficient swap and temporary space. Specifically:

- **Swap Space**–The system must have at least 512MB.
- **Temporary Space**–There must be a minimum of 2GB of free space in `/tmp`.

9.4 Meeting Operating System Requirements

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

1. Install a certified operating system.
2. Install all necessary patches and packages as listed in the *Release Notes for Identity Management*.
3. Review the *Oracle Fusion Middleware System Requirements and Specifications* and ensure that the Operating System requirements are met.

This section includes the following topics:

- Section 9.4.1, "Configuring Kernel Parameters."
- Section 9.4.2, "Setting the Open File Limit."
- Section 9.4.3, "Setting Shell Limits."
- Section 9.4.4, "Validating Local Hosts File."
- Section 9.4.5, "Increasing Huge Page Allocation for Exalogic Deployments."

9.4.1 Configuring Kernel Parameters

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

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

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

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

Table 9–1 UNIX Kernel Parameters

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

To set these parameters:

1. Log in as `root` and add or amend the entries in the file `/etc/sysctl.conf`. If the specified parameters do not exist in the file, then add the same.
2. Save the file.
3. Activate the changes by issuing the command:

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

9.4.2 Setting the Open File Limit

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

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

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

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

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

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

9.4.3 Setting Shell Limits

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

Most Linux Versions

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

Add the following lines:

```
* soft  nofile  150000
* hard  nofile  150000
* soft  nproc   4096
* hard  nproc   16384
```

Oracle Linux 6 and Red Hat Enterprise Linux 6 Only

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

Add the following lines:

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

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

Add the following lines:

```
* soft  nproc   4096
* hard  nproc   16384
```

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

After editing the file, reboot the machine.

9.4.4 Validating Local Hosts File

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

`IP_Address Fully_Qualified_Name Short_Name`

For example:

```
192.168.30.1 oimhost1vhn1.example.com oimhost1vhn1

192.168.30.2 oimhost2vhn1.example.com oimhost2vhn1

192.168.30.3 oimhost1vhn2.example.com oimhost1vhn2

192.168.30.4 oimhost2vhn2.example.com oimhost2vhn2

192.168.30.5 oimhost1vhn3.example.com oimhost1vhn3

192.168.30.6 oimhost2vhn3.example.com oimhost2vhn3

192.168.50.1 idstore.example.com idstore

192.168.50.2 igdinternal.example.com igdinternal

192.168.10.1 iamhost1.example.com iamhost1

192.168.10.2 iamhost2.example.com iamhost2

192.168.10.1 webhost1.example.com webhost1

192.168.10.2 webhost2.example.com webhost2
```

The exact entries that appear in the `/etc/hosts` file is dependent on how you are resolving your names, be it local host or DNS. The importance of this step is to validate the format of any entries which do appear in the file.

9.4.5 Increasing Huge Page Allocation for Exalogic Deployments

By default, huge pages are enabled in Exalogic compute nodes. Verify the existing allocation by running.

```
grep Huge /proc/meminfo
```

Set the recommended Huge Page allocation to `25000`.

To set the Huge Page allocation, run the following command as root in the compute node:

```
echo 25000  > /proc/sys/vm/nr_hugepages
```

9.5 Enabling Unicode Support

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

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

Set the LANGUAGE environment variable as follows:

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

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

9.6 Setting the DNS Settings

Configure the host to access your corporate DNS hosts. To do this, update DNS settings by updating the file `/etc/resolv.conf`.

9.7 Configuring Users and Groups

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

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

Groups

You must create the following groups on each node.

- `oinstall`
- `dba`

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

```
groupadd groupname
```

For example

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

User

You must create the following user on each node.

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

  Notes:

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

To create a local user, use the following command as `root`:

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

For example:

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

Note: To create this user in NIS, refer to your NIS documentation.

9.8 Configuring a Host to Use an NTP (time) Server

All servers in the deployment must have the same time. The best way to achieve this is to use an NTP server. To configure a host to use an NTP server:

1. Determine the name of the NTP server(s) you wish to use. For security reasons, ensure that these are inside your organization.
2. Log in to the host as the root user.
3. Edit the file `/etc/ntp.conf` to include a list of the time servers. After editing, the file appears as follows:

   ```
   server ntphost1.example.com
   server ntphost2.example.com
   ```

4. Run the following command to synchronize the system clock to the NTP server:

   ```
   /usr/sbin/ntpdate ntpserver1.example.com
   /usr/sbin/ntpdate ntpserver2.example.com
   ```

5. Start the NTP client using the following command:

   ```
   service ntpd start
   ```

6. Validate that the time is set correctly using the date command.
7. To make sure that the server always uses the NTP server to synchronize the time. Set the client to start on reboot by using the following command:

   ```
   chkconfig ntpd on
   ```

9.9 Configuring a Host to Use an NIS/YP Host

If you are using NFS Version 4, configure a directory service or an NIS (Network Information Server). If your organization does not have one already, use the built-in one on the ZFS storage appliance. See Configuring NFS Version 4 (NFSv4) on Exalogic in the *Oracle Fusion Middleware Exalogic Machine Owner's Guide* for more information.

Once you have configured your NIS host, configure each compute node to use it. Before beginning, determine the host names of the NIS servers you are going to use.

1. Login to the host as root.
2. Edit the `/etc/idmapd.conf` configuration file:

   ```
   vi /etc/idmapd.conf
   ```

   Set the domain value, as in the following example:

   ```
   Domain = example.com
   ```

3. Restart the `rpcidmapd` service:

   ```
   service rpcidmapd restart
   ```

4. Update the `/etc/yp.conf` configuration file, and set the correct domain value, as in the following example:

   ```
   vi /etc/yp.conf
   ```

   Add the following line:

   ```
   domain example.com server NIS_Server_hostname_or_IP
   ```

   Where `example.com` is the example domain and *NIS_Server_hostname_or_IP* is the host name or IP address of the NIS host. You must replace these sample values with values appropriate for your environment.

5. Set NIS domain name on the command line:

   ```
   domainname NIS_DOMAIN_NAME
   ```

   For example:

   ```
   domainname nisdomain.example.com
   ```

6. Edit the `/etc/nsswitch.conf` configuration file:

   ```
   vi /etc/nsswitch.conf
   ```

   Change the following entries:

   ```
   passwd:     files nis
   shadow:     files nis
   group:      files nis
   automount:  files nis nisplus
   aliases:    files nis nisplus
   ```

7. Restart the `rpcidmapd` service:

   ```
   service rpcidmapd restart
   ```

8. Restart the `ypbind` service by running the following command:

   ```
   service ypbind restart
   ```

9. Check the `yp` service by running this command:

```
ypwhich
```

10. Verify if you can access Oracle user accounts:

```
ypcat passwd
```

11. Add `ypbind` to your boot sequence, so that it starts automatically after rebooting.

```
chkconfig ypbind on
```

9.10 Enabling Virtual IP Addresses

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

This section includes the following topics:

- Section 9.10.1, "Summary of the Required Virtual IP Addresses"
- Section 9.10.2, "Enabling a Virtual IP Address on a Network Interface"
- Section 9.10.3, "Verifying the Required Virtual IP Addresses on the Network"

9.10.1 Summary of the Required Virtual IP Addresses

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

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

Check that the virtual host is enabled as follows:

Table 9–2 Logical Virtual IP Addresses Associated with IPoIB Network interfaces

VIP Values	Enabled on Host (Distributed)	Enabled on Host (Consolidated)
IADADMINVHN.example.com	OAMHOST1	IAMHOST1
IGDADMINVHN.example.com	OIMHOST1	IAMHOST2
OIMHOST1VHN1.example.com	OIMHOST1	IAMHOST1
OIMHOST1VHN2.example.com	OIMHOST1	IAMHOST1
OIMHOST1VHN3.example.com	OIMHOST1	IAMHOST1
OIMHOST2VHN1.example.com	OIMHOST2	IAMHOST2
OIMHOST2VHN2.example.com	OIMHOST2	IAMHOST2
OIMHOST2VHN3.example.com	OIMHOST2	IAMHOST2

Note: Use The Distributed values for Exalogic Virtual.

Use the Consolidated values for Exalogic Physical.

9.10.2 Enabling a Virtual IP Address on a Network Interface

This section describes how to enable a virtual IP address on a network interface. The procedure varies, depending on whether you are using Oracle Enterprise Linux 5 or Oracle Enterprise Linux 6.

Oracle Enterprise Linux 5

If you are using Oracle Enterprise Linux 5, complete the following steps to enable the virtual IP addresses listed in Table 9–2:

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

   ```
   ifconfig subinterface virtual_ip_address netmask netmask_value
   ```

   For example, to enable the IP address 192.168.20.3, net mask 255.255.240 on network card bond0, use the following command:

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

   Note: The example in this section is applicable for both physical and virtual Exalogic deployments.

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

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

   This command does not return a response. The section Section 9.10.3, "Verifying the Required Virtual IP Addresses on the Network" describes how to verify if the commands have worked.

Oracle Enterprise Linux 6 or Later

Starting with Oracle Enterprise Linux 6, the `ifconfig` command is deprecated and is replaced with the `ip` command. To enable the virtual IP addresses listed in Table 9–2 on Oracle Enterprise Linux 6 or later, complete the following steps:

1. Determine the CIDR notation of the netmask. Each Netmask has a CIDR notation. For example, `255.255.240.0` has a CIDR of `20`.

   If the netmask you are adding is the same as the interface, the fastest way to determine this is to examine the existing IP address assigned to the network card. You can do this using the following command:

   ```
   ip addr show dev bond0
   ```

   The following is a sample output:

   ```
   2: bond0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:21:f6:03:85:9f brd ff:ff:ff:ff:ff:ff
   int 192.168.20.1/20 brd 10.248.11.255 scope global bond0
   ```

   In this example, the CIDR value is the value after `/`, that is, `20`. If you are unsure of the CIDR value, contact your network administrator.

2. Add the IP address `192.168.20.3`, net mask `255.255.240` (CIDR20) on network card `bond0` using the following command:

   ```
   ip addr add 192.168.20.3/20 dev bond0:1
   ```

3. For each of the virtual IP addresses you define, update the ARP caches using the following command:

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

> **Note:** Due to a known issue in the `ifconfig` utility, during server migration, all VIPs are dropped from the network interface on the machine the WebLogic Managed Server is migrated from. This happens when the VIP is enabled on `:0` of the network interface. To workaround the issue, enable the VIPs on the network interface starting with `:1`.

9.10.3 Verifying the Required Virtual IP Addresses on the Network

Check that each node can communicate with each other node using both physical and virtual host names for example:

```
ping IADADMINVHN.example.com
ping IGDADMINVHN.example.com
ping OIMHOST1VHN1.example.com
ping OIMHOST1VHN2.example.com
ping OIMHOST1VHN3.example.com
ping OIMHOST2VHN1.example.com
ping OIMHOST2VHN2.example.com
ping OIMHOST2VHN3.example.com
```

9.11 Mounting Shared Storage onto the Host

As shown in Chapter 7, "Preparing Storage for an Enterprise Deployment," you must make shared storage available to each host that will use it.

This section includes the following topics:

- Section 9.11.1, "Mounting Shared Storage"
- Section 9.11.2, "Validating the Shared Storage Configuration"

9.11.1 Mounting Shared Storage

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

> **Note:** The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from OAMHOST1. The options may differ depending on the specific storage device.
>
> ```
> mount -t nfs -o
> rw,bg,hard,nointr,proto=tcp,vers=3,timeo=300,rsize=32768,wsize=3276
> 8 nasfiler:VOL1/OracleIAM /u01/oracle
> ```
>
> Contact your storage vendor and machine administrator for the correct options for your environment.

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

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

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

For example:

```
mount -t nfs nasfiler:/export/IAM/binaries  /u01/oracle/products
```

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

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

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

For NFS 3:

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

For NFS 4:

```
nasfiler:VOL1/OracleIAM /u01/oracle nfs4
rw,bg,hard,nointr,timeo=300,noaci,rsize=131072,wsize=131072,proto=tcp
```

9.11.2 Validating the Shared Storage Configuration

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

For example:

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

Verify that the owner and permissions are correct:

```
ls -l testfile
```

Then remove the file:

```
rm testfile
```

10

Preparing the Database for an Enterprise Deployment

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

This chapter contains the following topics:

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

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

- Verify the database requirements as described in Section 10.2, "Verifying the Database Requirements for an Enterprise Deployment."
- Install and configure the Oracle database repositories. See the installation guides listed in the "Related Documents" section of the Preface and Section 10.3, "Installing the Database for an Enterprise Deployment."
- Create database services, as described in Section 10.4, "Creating Database Services."
- Create the required Oracle schemas in the database using the Repository Creation Utility (RCU). See Section 10.7, "Loading the Identity and Access Management Schemas in the Oracle RAC Database Using RCU."

10.2 Verifying the Database Requirements for an Enterprise Deployment

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

- Section 10.2.1, "Databases Required"
- Section 10.2.2, "Database Host Requirements"
- Section 10.2.3, "Database Versions Supported"
- Section 10.2.4, "Patch Requirements for Oracle Database 11g (11.2.0.2.0)"
- Section 10.2.5, "Oracle Database Minimum Requirements"

10.2.1 Databases Required

For Oracle Identity and Access Management, a number of separate databases are recommended. Table 10–1 provides a summary of these databases. Which database or databases you use depends on the topology that you are implementing.

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

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

Table 10–1 Mapping between Databases and Schemas

Database Names	Database Hosts	Scan Address	Service Name	RCU Prefix	Schemas in Database
IADDB	IADDBHOST1 IADDBHOST2	*IADDBSCAN*	`iadedg.example.com`	EDGIAD	OAM, IAU, MDS, OPSS, MSM, OIF
IGDDB	IGDDBHOST1 IGDDBHOST2	*IAMDBSCAN*	`OIMEDG.example.com`	EDGIGD	OIM, SOAINFRA, MDS, OPSS, ORASDPM, BI, ODS

Note: Table 10–1 shows two separate database to make the transition to a multi data center deployment simpler. You may combine two databases into a single database, if required.

Note: ODS is required only if you are using OID. This can be placed into a dedicated database if required

The following sections apply to all the databases listed in Table 10–1.

10.2.2 Database Host Requirements

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

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

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

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

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

10.2.3 Database Versions Supported

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

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

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

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

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

10.2.4 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

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

Table 10–2 lists the patches required for Oracle Identity Manager configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 10–2 Required Patches for Oracle Database 11g (11.2.0.2.0)

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

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

Note:

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

10.2.5 Oracle Database Minimum Requirements

The Oracle Database must meet some minimum requirements.

10.2.5.1 General Database Characteristics

- Character Set–The character set must be Unicode compliant, for example: AL32UTF8.
- Database Options–The following database options must be installed into the database:
  - Oracle JVM
  - Oracle Text
- Database Views–The following Database view must be created on the database:
  - XAVIEWS
- Database Packages–The following Database package must exist in the database:
  - DBMS_SHARED_POOL
- Transparent Data Encryption - This is required by Oracle Privileged Account Manager

10.2.5.2 Minimum Initialization Parameters

The databases must have the following minimum initialization parameters defined:

Table 10–3 Minimum Initialization Parameters for Oracle Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	1600
session_max_open_files	50
sessions	500
processes	500
sga_target	550M
pga_aggregate_target	110M
sga_max_size	4G
session_cached_cursors	500

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

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

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

```
srvctl stop database -d iaddb
srvctl start database -d iaddb
```

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

10.3 Installing the Database for an Enterprise Deployment

Install and configure the database repository as follows.

Oracle Clusterware

- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- 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 11*g* Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

Oracle Real Application Clusters Database

Create a Real Applications Clusters Database with the following characteristics:

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

10.4 Creating Database Services

When multiple Oracle Fusion Middleware products are sharing the same database, each product should be configured to connect to a separate, dedicated database service.

Note: The instructions in this section are for the Oracle Database 12c (12.1) release. If you are using another supported database, refer to the appropriate documentation library for more up-to-date and release-specific information.

For more information about connecting to Oracle databases using services, see "Overview of Using Dynamic Database Services to Connect to Oracle Databases" in the *Oracle Real Application Clusters Administration and Deployment Guide*.

In addition, the database service should be different from the default database service. For complete instructions on creating and managing database services for an Oracle Database 12c database, see "Overview of Automatic Workload Management with Dynamic Database Services" in the *Oracle Real Application Clusters Administration and Deployment Guide*.

Run-time connection load balancing requires configuring Oracle RAC Load Balancing Advisory with service-level goals for each service for which load balancing is enabled.

This section includes the following topics:

- Section 10.4.1, "Creating Database Services for 12c Databases"
- Section 10.4.2, "Creating a Database Service for Oracle Internet Directory"

10.4.1 Creating Database Services for 12*c* 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 10–1, " Mapping between Databases and Schemas".

1. Log in to SQL*Plus and create the service:

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

```
SQL> EXECUTE DBMS_SERVICE.CREATE_SERVICE
(SERVICE_NAME => 'iadedg.example.com',
NETWORK_NAME => 'iadedg.example.com'
);
```

> **Note:** For the Service Name of the Oracle RAC database, use lowercase letters, followed by the domain name. For example:
>
> `iadedg.example.com`
>
> Enter the `EXECUTE DBMS_SERVICE` command shown on a single line.
>
> For more information about the `DBMS_SERVICE` package, see *Oracle Database PL/SQL Packages and Types Reference*.

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

```
srvctl add service -d iaddb -s iadedg.example.com -r iaddb1,iaddb2 -q FALSE -m
NONE -e SELECT -w 0 -z 0
```

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

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

3. Start the Service using `srvctl start service`

```
srvctl start service -d iaddb -s iadedg.example.com
```

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

```
srvctl status service -d iaddb -s iadedg.example.com
Service iadedg.example.com is running on instance(s) iaddb1,iaddb2
```

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

```
srvctl config service -d iaddb -s iadedg.example.com
Service name: iadedg.example.com
Service is enabled
Server pool: IADDB_iadedg.example.com
Cardinality: 2
Disconnect: false
Service role: PRIMARY
Management policy: AUTOMATIC
DTP transaction: false
AQ HA notifications: false
Failover type: SELECT
Failover method: NONE
TAF failover retries: 0
TAF failover delay: 0
Connection Load Balancing Goal: LONG
Runtime Load Balancing Goal: NONE
TAF policy specification: NONE
Edition:
Preferred instances: iaddb1,iaddb2
Available instances:
```

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

10.4.2 Creating a Database Service for Oracle Internet Directory

OID does not have the same retry logic as Weblogic Grid Link Datasources. However creating a database service specifically for OID which is TAF (Transparent Application Failover) enabled, will simulate this logic and result in faster resumption after the failure of a database RAC instance.

To create a TAF enabled database service, issue the following commands:

```
srvctl add service -d igddb -s oidedg.example.com -r igddb1,igddb2 -q
TRUE -m BASIC -e SELECT -w 5 -z 5

srvctl start service -d igddb -s oidedg.example.com

srvctl status service -d igddb -s oidedg.example.com
```

Note: In the above commands, `iamdb`, `oidedg.example.com`, `iamdb1`, `iamdb2`, and `idmdb` are sample values. You must substitute them with the appropriate values.

10.5 Using SecureFiles for Large Objects (LOBs) in an Oracle Database

Beginning with Oracle Database 11*g* Release 1, Oracle introduced SecureFiles, a new LOB storage architecture. It is recommended that you use SecureFiles for the Oracle Fusion Middleware schemas, in particular, for the Oracle SOA Suite schemas. For

more information, see "SecureFiles LOB Storage" in the *Oracle Database SecureFiles and Large Objects Developer's Guide*.

In Oracle 12*c* Database, the default setting for using SecureFiles is `PREFERRED`. This means that, the database attempts to create a SecureFiles LOB unless a BasicFiles LOB is explicitly specified for the LOB or the parent LOB (if the LOB is in a partition or sub-partition). The Oracle Fusion Middleware schemas do not explicitly specify BasicFiles, which means that, Oracle Fusion Middleware LOBs will default to SecureFiles when installed in an Oracle 12*c* database.

For Oracle 11*g* databases, the `db_securefile` system parameter controls the SecureFiles usage policy. This parameter can be modified dynamically. The following options can be used for using SecureFiles:

- `PERMITTED`: This options allows SecureFiles to be created. This is the default setting for db_securefile. The default storage method uses BasicFiles.
- `FORCE`: This option creates all new LOBs as SecureFiles.
- `ALWAYS`: This option tries to create LOBs as SecureFiles, but falls back to BasicFiles if not possible (that is, if ASSM is disabled).
- `IGNORE`: This option ignores attempts to create SecureFiles.
- `NEVER`: This option disallows new SecureFiles creations.

For Oracle 11*g* Databases, it is recommended that you set the `db_securefile` parameter to `FORCE` before creating the Oracle Fusion Middleware schemas using the Repository Creation Utility (RCU).

> **Note:** The SecureFiles segments require tablespaces managed with automatic segment space management (ASSM). This means that, LOB creation on SecureFiles will fail if ASSM is not enabled. However, the Oracle Fusion Middleware tablespaces are created by default with ASSM enabled. As a result, with the default configuration, nothing needs to be changed to enable SecureFiles for the Oracle Fusion Middleware schemas.

10.6 Database Tuning

The database parameters defined in Section 10.2.5.2, "Minimum Initialization Parameters" are only a guide. You might need to perform additional tuning after the system is in use. For more information, see *Database Performance Tuning Guide*.

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

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

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

This section describes the list of schemas required for deploying Identity and Access Management and the procedure for creating it manually. This section includes the following topics:

10.7.1 Schemas Required by Identity and Access Management

Before you can configure the Oracle Identity and Access Management software, you must install the database schemas listed in Table 10–4.

If you are using the IDMLCM provisioning tool to automatically configure the software, then you can create these schemas as part of the automated deployment.

If you wish to create the schemas manually, then follow the instructions described in Section 10.7.2, "Creating the Database Schemas Manually".

Table 10–4 Database Schemas Required for Oracle Identity and Access Management

Database	RCU Prefix	Product	RCU Option	Comments
IADDB	EDGIAD	Oracle Platform Security Services for IAMAccessDomain	AS Common Schemas–Oracle Platform Security Service	Audit and Metadata Services are also selected.
IADDB	EDGIAD	Oracle Access Management Access Manager	Identity Management–Oracle Access Manager	Audit Services will also be selected.
IADDB	EDGIAD	Oracle Adaptive Access Manager	Oracle Identity Management–Oracle Adaptive Access Manager	If required.
IGDDB	EDGIGD	Oracle Platform Security Services for IAMGovernanceDomain	AS Common Schemas–Oracle Platform Security Service	Audit and Metadata Services are also selected.
IGDDB	EDGIGD	Oracle Identity Manager	Identity Management–Oracle Identity Manager	Metadata Services, SOA infrastructure, and User Messaging will also be selected.
IGDDB	EDGIGD	Oracle Privileged Account Manager	Oracle Identity Management - Oracle Privileged Account Manager	
IGDDB	EDGIGD	Oracle Business Intelligence	Oracle Identity Management - Oracle Business Intelligence Manager	
IGDDB	EDGIGD	Oracle Internet Directory	Oracle Identity Management - Oracle Internet Directory	If you are using internet directory.

Note: Although you are specifying a prefix for OID, OID will not actually use a prefix. This is a limitation of the tool.

> **Note:** While it is recommended to separate schemas into different databases to aid with future Multi Data Center deployments, it is not mandatory to do so, and if you have no plans to use Multi Data Center, it may be better to place all schemas in a single database.

When creating schemas manually using Repository Creation Utility (RCU), you must select the following products in Select Components screen of RCU:

- For Oracle Identity Manager, select **Identity Management - Oracle Identity Manager**.
- For Oracle Access Manager, select the following:
  - **Identity Management - Oracle Access Manager**
  - **Identity Management - Oracle Mobile Security Manager**
  - **Identity Management - Oracle Adaptive Access Manager** - if Oracle Adaptive Access Manager (OAAM) is part of your deployment.

> **Note:** When you select **Oracle Identity Management** or **Oracle Access Management** under **Identity Management**, all the required schema components for the selected product are selected automatically.

10.7.2 Creating the Database Schemas Manually

This section describes how to create schemas manually using the Repository Creation Utility.

You must to run the Repository Creation Utility (RCU) twice, once for each domain specifying a different Prefix each time. To create the schemas, complete the following steps:

1. Start the Repository Creation Utility (RCU) by issuing this command:

   RCU_ORACLE_HOME`/bin/rcu`

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

   Database Type: `Oracle Database`

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

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

   - **Username:** `sys`

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

Click **Next**.

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

   Create a New Prefix: Enter a prefix to be added to the database schemas. Note that all schemas are required to have a prefix. See Table 10–1, " Mapping between Databases and Schemas" or Table 10–4, " Database Schemas Required for Oracle Identity and Access Management" for RCU prefixes.

   Components: Select the appropriate components from the Table 10–4 for the topology you are using.

   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 10–1 in this chapter provides the recommended mapping between the schemas and their corresponding databases. Refer to this table to ensure that the correct details are entered in this screen.

   ---

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. The deployment wizard requires that all passwords for a given prefix be the same.

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

    Click **Close** to exit.

10.8 Backing up the Database

After you have prepared your database, back it up as described in Section 31.5.3.3, "Backing Up the Database."

Part III

Configuring an Oracle Identity and Access Management Enterprise Deployment Manually

Use this part of the guide to configure the Oracle Identity and Access Management software manually, using the standard Oracle Fusion Middleware installers, Repository Creation Utility, and Configuration Wizard, as well as custom configuration tools required for Identity and Access Management.

For information about automating the configuration process, see Part IV, "Configuring an Enterprise Deployment Using Life Cycle Management (LCM) Tools".

This part contains the following chapters:

11

Installing Oracle Fusion Middleware in Preparation for an Enterprise Deployment

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

This chapter contains the following topics:

11.1 Overview of the Software Installation Process

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.

> **See Also:** *Oracle Fusion Middleware Download, Installation, and Configuration Readme* for this release.

This section includes the following topics:

11.1.1 Software to Install

Different topologies use different servers and require different software to be installed. For information about the different enterprise deployment topologies, see Chapter 2, "Understanding the IAM Enterprise Deployment".

The subsequent sections explain how to install various software.

Where two different pieces of Oracle binary software are installed onto the same host (for example OIM11g and SOA11g), this software is installed in the same Middleware home location, but in different Oracle homes.

Notes:

- When 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`.

Note: ■OHS is required for on-premise and Exalogic deployments with an external OHS.

- OTD is only required if you are installing on Exalogic.
- OUD is only required if you are creating a new OUD directory.
- IDM is only required if you are creating a new OID directory.
- If you are performing an automated deployment using IDM Life Cycle Management (LCM) tool, you must install LDAP directory and Oracle Traffic Director if deploying on Exalogic.

For more information on various Middleware homes (MW_HOME), refer to Chapter 7, "Preparing Storage for an Enterprise Deployment".

Oracle Identity Management products are bundled as two product sets: Oracle Identity Management and Oracle Identity and Access Management. (See Software versions). The relevant Identity Management software is installed into separate Oracle homes.

11.1.2 Summary of Homes

Oracle binaries are installed into an Oracle Fusion Middleware home. Individual products are installed into Oracle homes within the Middleware home. Table 11–1 is a summary of the Middleware homes and Oracle homes used in this document.

Table 11–1 Summary of Homes

Home Name	Home Description	Products Installed
IAD_MW_HOME	The Oracle Middleware Home containing the ORACLE_HOMEs required by Oracle Identity Manager.	
IGD_MW_HOME	The Oracle Middleware Home containing the ORACLE_HOMEs required by Oracle Access Manager.	
DIR_MW_HOME	The Oracle Middleware Home containing the ORACLE_HOMEs required by Oracle Unified Directory.	

Table 11–1 (Cont.) Summary of Homes

Home Name	Home Description	Products Installed
WL_HOME	This is the root directory in which Oracle WebLogic Server is installed. The WL_HOME directory is a peer of Oracle home directory and resides within the MW_HOME.	Oracle WebLogic Server
JAVA_HOME	Contains the Oracle Java installation. This is the jdk installed in the *MW_HOME* when the *MW_HOME* was created. This will be the version in *REPOS_HOME*/jdk when invoking the Oracle Universal Installer (runInstaller).	
IAD_ORACLE_HOME	Contains the binary and library files required for Oracle Identity and Access Management and is located in IAD_MW_HOME/iam.	Access Manager
OUD_ORACLE_HOME	Contains the binary and library files required for Oracle Unified Directory and is located in *MW_HOME*/oud.	Oracle Unified Directory
IGD_ORACLE_HOME	Contains the binary and library files required for Oracle Identity and Access Management and is located in *IGD_MW_HOME*/iam.	Oracle Identity Manager
OUD_ORACLE_HOME	Contains the binary and library files required for Oracle Unified Directory and is located in *DIR_MW_HOME*/oud.	Oracle Unified Directory
OID_ORACLE_HOME	Contains the binary and library files required for Oracle Unified Directory and is located in *DIR_MW_HOME*/oid.	
SOA_ORACLE_HOME	Contains the binary and library files required for the Oracle SOA Suite. Located in *IGD_MW_HOME*/soa.	Oracle SOA Suite
ORACLE_COMMON_HOME	Contains the generic Oracle home files. This Oracle home is created automatically by any product installation and is located in *MW_HOME*/oracle_common.	Generic commands
LCM_HOME	Lifecycle Repository.	
REPOS_HOME	Software Repository.	
WEB_MW_HOME	The Oracle Middleware Home containing the ORACLE_HOMEs required by the web tier.	
OHS_ORACLE_HOME	Contains the binary and library files required for Oracle HTTP server.	
WEBGATE_ORACLE_HOME	Contains the binaries for Oracle WebGate and is located in *WEB_MW_HOME*/web.	Oracle WebGate
MSAS_ORACLE_HOME	Contains the binary and library files required by Mobile Security Access Server	
OTD_WEBGATE_ORACLE_HOME	Contains the binary and library files required for Oracle Traffic Director.	
OTD_WEBGATE_ORACLE_HOME	Contains the binaries for Oracle WebGate for Oracle Traffic Director and is located in *WEB_MW_HOME*.	

11.2 Installing the Web Tier

This section describes how to install the Web tier:

This section contains the following topics:

- Section 11.2.1, "Installing Oracle HTTP Server"
- Section 11.2.2, "Installing Oracle Traffic Director"
- Section 11.2.3, "Installing Oracle Mobile Security Access Server"

11.2.1 Installing Oracle HTTP Server

This section and the ones following provide a brief overview of how to install Oracle Traffic Director and the Oracle Fusion Middleware Software.

> **Note:** If you are using IDM Life Cycle Management (LCM) tool for deploying Oracle Identity and Access Management, skip this task.

This section explains how to install Oracle HTTP Server on WEBHOST1 and WEBHOST2.

This section contains the following topics:

- Section 11.2.1.1, "Running the Installer"
- Section 11.2.1.2, "Backing Up the Installation"

11.2.1.1 Running the Installer

As described in Section 7, "Preparing Storage for an Enterprise Deployment," you install the Oracle HTTP Server onto a private 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.

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

- `LD_ASSUME_KERNEL`
- `ORACLE_INSTANCE`

To start Oracle Universal Installer on Linux, go to the following directory:

REPOS_HOME`/installers/webtier/Disk1`

Run the following command:

```
./runInstaller
```

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 Software –> 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:

     WEB_MW_HOME

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

6. On the Specify Security Updates 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**.

11.2.1.2 Backing Up the Installation

Back up the Fusion Middleware Home now (make sure no server is running at this point).

11.2.2 Installing Oracle Traffic Director

This section describes how to install Oracle Traffic Director software on WEBHOST1 and WEBHOST2. This step is required only if you are deploying on Oracle Exalogic.

Note: Be sure that you are not logged in as root user before installing or performing any action on Oracle Traffic Director.

Note: Be sure to verify you have obtained all required patches. For more info, see *Release Notes for Oracle Identity and Access Management*.

To install Oracle Traffic Director:

1. Extract the contents of the installer zip file to a directory on WEBHOST1. It is recommended that this location is *REPOS_HOME*`/installers/otd`.

2. Change directory to the `Disk1` subdirectory in the directory in which you unzipped the installer.

3. Set the `DISPLAY` in your machine if not already done, and then run the following command:

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

4. Follow the instructions on the screen to install the software.

   When the Specify Installation Location screen appears, enter the value of the *OTD_ORACLE_HOME* variable in the **Oracle Home Directory** field.

   The recommended directory location for the *OTD_ORACLE_HOME* is listed in Table 7–4, " Private Storage Directories - Distributed Topology"

If you need help with any of the other options on the installer screens, click **Help**, or refer to "Installing Oracle Traffic Director in Graphical Mode" in the *Oracle Traffic Director Installation Guide*.

5. If you are using Private or Local Storage for your web tier binaries, repeat steps 1 through 4 on WEBHOST2.

Note: If this is the first time you have installed any software on this host, you may be asked to create an inventory location file.

To create an inventory location, run the following command as root:

```
REPOS_
HOME/installers/otd/Disk1/stage/Response/createCentralInvent
ory.sh SW_ROOT oinstall
```

In this command, `oinstall` is the name of the group you created in Section 13.5.2, "Creating Users and Groups".

11.2.3 Installing Oracle Mobile Security Access Server

This section explains how to install Oracle Mobile Security Access Server (MSAS) on WEBHOST1 and WEBHOST2.

Note: If you are deploying Oracle Identity and Access Management using IDM LCM tool, or if you do not require Oracle Mobile Security Suite, skip this task.

As described in Section 7, "Preparing Storage for an Enterprise Deployment," you install the MSAS onto a private disk.

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

- `LD_ASSUME_KERNEL`
- `ORACLE_INSTANCE`

To install MSAS:

1. Start the installer using the following command:

   ```
   cd REPOS_HOME/installers/omsas/Disk1
   ./runInstaller -jreLoc $JAVA_HOME
   ```

   If the `$JAVA_HOME` is not set, replace `$JAVA_HOME` with the absolute path to the Java home.

2. 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 and click **Next**.
   - Follow the instructions on screen to execute `createCentralInventory.sh` as `root` and click **OK**.
3. On the Welcome screen, click **Next**.

4. On the install Software Updates Screen choose to either search for updates by entering you're my Oracle support account details or select **Skip Software Updates** and click **Next**.
5. On the Prerequisite Checks screen, if all the pre-checks have completed successfully, click **Next**.
6. On the Specify Installation Location screen, specify the following values:
   - **Fusion Middleware Home Location (Installation Location)** For example:

     WEB_MW_HOME

   - Oracle Home Location Directory: `omsas`

   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**.
8. In the Installation Complete Screen click **Finish**.
9. Back up the installation (*WEB_MW_HOME*).

11.3 Creating an Oracle Fusion Middleware Home

As described in Chapter 7, "Preparing Storage for an Enterprise Deployment," you install Oracle Fusion Middleware software in at least two storage locations for redundancy.

- Section 11.3.1, "Installing a Supported JDK"
- Section 11.3.2, "Installing Oracle WebLogic Server"

11.3.1 Installing a Supported JDK

Perform the following tasks to install a supported JDK:

1. Section 11.3.1.1, "Identifying and Downloading the JDK Software"
2. Section 11.3.1.2, "Installing JDK"

11.3.1.1 Identifying and Downloading the JDK Software

To identify a certified JDK for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0), see the certification document for 11*g* Release 2 (11.1.2.3.0) on the *Oracle Fusion Middleware Supported System Configurations* page.

After you identify the supported Oracle JDK, download it from the following location on Oracle Technology Network:

`http://www.oracle.com/technetwork/java/index.html`

Make sure that you navigate to the download for the Java SE JDK.

> **Note:** If you have downloaded the software repository, Java will be included in it.

Copy the downloaded zip file to the location *REPOS_HOME*`/installers/jdk`.

11.3.1.2 Installing JDK

This section describes how to install JDK.

> **Note:** If you are performing an automated deployment using IDM LCM tool, then this step is only necessary if you need to create an Oracle LDAP directory.

To install the JDK you downloaded in the earlier sections, or to install the JDK that is available in the software repository, complete the following steps:

1. Create a new directory `MW_HOME` using the following command:

   ```
   mkdir MW_HOME
   ```

   In this command, `MW_HOME` is the *`MW_HOME`* you are creating. For example, *`IAD_MW_HOME`*.

2. Change directory to `MW_HOME`.
3. Do one of the following:
   - Unzip the JDK from the software repository using the following command:

     ```
     unzip REPOS_HOME/installers/jdk/jdk.zip
     ```

     OR
   - Extract the jdk from the downloaded tar file using the following command:

     ```
     tar -xzvf REPOS_HOME/installers/jdk/jdk-7u55-linux-x64.tar.gz
     ```

   This creates a directory named `jdk_version`. To reduce confusion in the future if your java is upgraded, it is recommended to rename this directory to simply `jdk` or to create a symbolic link from `jdk_version` to `jdk`.
4. Install the JDK in the following MW_HOME directories:
   - *`IAD_MW_HOME`* install from OAMHOST1
   - *`IGD_MW_HOME`* install from OIMHOST1
   - *`DIR_MW_HOME`* install from LDAPHOST1
5. Validate the installation by running the following command:

   ```
   set JAVA_HOME to MW_HOME/jdk
   ```

   Add `JAVA_HOME` to your `PATH` variable.
6. Run the following command to verify that the appropriate java executable is in the PATH, and your environment variables are set correctly:

   ```
   java -version
   ```

   Sample Output:

   ```
   java version "1.7.0_55"
   Java(TM) SE Runtime Environment (build 1.7.0_55-b13)
   Java HotSpot(TM) 64-Bit Server VM (build 24.55-b03, mixed mode)
   ```

11.3.2 Installing Oracle WebLogic Server

Perform these steps to install the Oracle WebLogic Server.

Install the WebLogic Server in the following MW_HOME directories:

- *IAD_MW_HOME* install from OAMHOST1
- *IGD_MW_HOME* install from OIMHOST1
- *DIR_MW_HOME* install from LDAPHOST1

To install WebLogic Server:

1. Add Java to your system path using the following command:

   ```
   export PATH=MW_HOME/jdk/bin:PATH
   ```

   Where `MW_HOME` is the *MW_HOME* into which you are installing the software. For example: *IAD_MW_HOME*.

2. Check the version of java using the following command:

   ```
   java -version
   ```

   Ensure that the 64-bit version is displayed if you are using a 64-bit operating system.

3. Start the WebLogic installer using the following command:

   ```
   cd REPOS_HOME/installers/weblogic
   java -d64 -jar wls_generic.jar
   ```

4. In the Welcome screen, click **Next**.
5. In the Choose Middleware Home Directory screen:
   - Select **Create a new Middleware Home**.
   - For Middleware Home Directory, enter *IAD_MW_HOME*

   Click **Next**.
6. In the Register for Security Updates screen, enter your contact information so that you can be notified of security updates. Click **Next**.

   Note: If you decide to be notified of security updates, the server will try to contact `www.oracle.com`; if it cannot do so, it may display a dialogue box asking you to provide proxy details to connect to the internet. Either enter these details which will be specific to your organization or check the box - **I wish to remain uniformed of security issues in my configuration or this machine has no internet access**.

7. In the Choose Install Type screen, select **Typical**, and click **Next**.
8. On the JDK Selection screen, select the jdk you added to your path in Step 1.

   It should be listed by default.

   Click **Next**.
9. In the Choose Product Installation Directories screen, accept the following directories:

   Middleware Home Directory: *IAD_MW_HOME*

   P**roduct Installation Directories for WebLogic Server:** *IAD_MW_HOME*`/wlserver_10.3`

   Oracle Coherence: *IAD_MW_HOME*`/coherence_3.7`

Click **Next**.

10. In the Installation Summary screen, click **Next**.

    The Oracle WebLogic Server software is installed.

11. In the Installation Complete screen, clear the **Run Quickstart** check box and click **Done**.

12. Repeat for Each Middleware Home.

11.4 Installing the Directory Tier

This section describes how to install the Directory Tier.

This section contains the following topics:

- Section 11.4.1, "Installing Oracle Unified Directory"
- Section 11.4.2, "Installing Oracle Internet Directory"

11.4.1 Installing Oracle Unified Directory

If you are creating a new Oracle Unified Directory, Install Oracle Unified Directory (OUD) into the *DIR_MW_HOME* on the host LDAPHOST1.

To install Oracle Unified Directory:

1. Start the Oracle Fusion Middleware 11*g* Oracle Unified Directory Installer using the following commands:

   ```
   cd REPOS_HOME/installers/oud/Disk1
   ./runInstaller -jreLoc $JAVA_HOME
   ```

   If `$JAVA_HOME` is not set, replace it with the location of the Java JDK. For example, *IGD_MW_HOME*`/jdk`

2. If displayed, on the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:

   - 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 and click **OK**.

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

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

   Click **Next**.

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

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

   - **OUD Base Location Home**: `/u01/oracle/products/dir (DIR_MW_HOME)`
   - **Oracle Home Directory**: Enter `oud` as the Oracle home directory name.

   Click **Next**.

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

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

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

11.4.2 Installing Oracle Internet Directory

If you are creating a new Oracle Internet Directory, Install Oracle Identity Management (IDM) into the *DIR_MW_HOME* on the host LDAPHOST1.

To install Oracle Internet Directory:

1. Start the Oracle Fusion Middleware 11g Oracle Internet Directory Installer using the following commands:

   ```
   cd REPOS_HOME/installers/idm/Disk1
   ./runInstaller -jreLoc JAVA_HOME
   ```

   Where *JAVA_HOME* is the location of the Java JDK for example *DIR_MW_HOME*/jdk

2. If displayed, on the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
   - 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 and click **OK**.
3. On the Welcome screen, click **Next**.
4. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.

   Click **Next**.
5. On the Select Installation Type screen, select **Install Software - Do Not Configure**, and then click **Next**.
6. On the Prerequisite Checks screen, verify that the checks complete successfully and click **Next**.
7. 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:

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

   Click **Next**.
8. On the Installation Summary screen, click **Install**.
9. On the Installation Progress screen, click **Next**.
10. On the Installation Complete screen, click **Finish**.
11. When the installation completes you are prompted to run the oracleRoot.sh script located in the *OID_ORACLE_HOME* directory:

    Run this script on LDAPHOST1 and LDAPHOST2 as the root user.

11.5 Installing the Application Tier

This section describes how to install the Application Tier.

This section contains the following topics:

- Section 11.5.1, "Installing Oracle Identity and Access Management"
- Section 11.5.2, "Installing Oracle SOA Suite"
- Section 11.5.3, "Creating the wlfullclient.jar File"

11.5.1 Installing Oracle Identity and Access Management

Oracle Identity and Access Management consists of the following products:

- Oracle Access Management Access Manager
- Oracle Identity Manager

Perform the steps in this section to install Oracle Identity and Access Management into the directories *IAD_MW_HOME* and *IGD_MW_HOME* on the hosts OAMHOST1 and OIMHOST1.

To install Oracle Identity and Access Management into *IGD_MW_HOME* perform the following steps:

1. Start the Oracle Fusion Middleware 11g Oracle Identity and Access Management using the following commands:

   ```
   cd REPOS_HOME/installers/iamsuite/Disk1
   ./runInstaller -jreLoc JAVA_HOME
   ```

   Where *JAVA_HOME* is the location of the Java JDK. For example, *IGD_MW_HOME*/jdk

2. If displayed, on the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
   - 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 and click **Next**.
3. On the Welcome screen 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/oracle/products/identity
   - **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**.
9. Repeat for each MW_HOME

11.5.2 Installing Oracle SOA Suite

Oracle SOA suite is only required if you are deploying Oracle Identity Governance. To Install Oracle SOA Suite into *IGD_MW_HOME*, perform the following steps on OIMHOST1.

Then perform these installation steps:

1. Start the Oracle Fusion Middleware 11g Oracle SOA Suite using the following commands:

   ```
   cd REPOS_HOME/installers/soa/Disk1
   ./runInstaller -jreLoc JAVA_HOME
   ```

   Where *JAVA_HOME* is the location of the Java JDK for example *IGD_MW_HOME*/jdk

2. If displayed, on the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
   - 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 and click **OK**.
3. On the Welcome screen, click **Next**.
4. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.

   Click **Next**.
5. On the Prerequisite Checks screen, verify that the checks complete successfully, and then click **Next**.
6. 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/oracle/products/identity (IGD_MW_HOME)*
   - **Oracle Home Directory**: Enter soa as the Oracle home directory name.
7. Click **Next**.
8. If the Application Server screen appears, click **Next**.
9. On the Installation Summary screen, click **Install**.
10. On the Installation Process screen, click **Next**.
11. On the Installation Complete screen, click **Finish**.

11.5.3 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 following directory on all the machines hosting Oracle Identity Manager in the application tier of your environment:

IGD_MW_HOME/wlserver_10.3/server/lib

To create the wlfullclient.jar file:

1. Navigate to the *IGD_MW_HOME*/wlserver_10.3/server/lib directory
2. Set your *JAVA_HOME* environment variable and ensure that the *JAVA_HOME*/bin directory is in your path.
3. Create the wlfullclient.jar using the following command:

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

11.6 Backing Up the Installation

Back up the Fusion Middleware Home now (make sure no server is running at this point).

11.7 Creating a Redundant Middleware Home

If you wish to create a redundant Middleware home to protect from binary corruptions, you can do so by following the steps described in Appendix A, "Creating a Redundant Middleware Home".

12

Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment

If you are creating a new Oracle LDAP directory, either Oracle Unified Directory (OUD) or Oracle Internet Directory (OID), you must create the directories. The instructions for this differ depending on whether you are configuring OUD or OID.

This chapter includes the following topics:

- Configuring Oracle Unified Directory
- Configuring Oracle Internet Directory

12.1 Configuring Oracle Unified Directory

Oracle Unified Directory is an optional component in an Identity Management Enterprise Deployment. You can use it as the Identity Store, that is, for storing information about users and groups.

In this section, you configure two instances of Oracle Unified Directory by using Oracle Unified Directory configuration assistant.

- Section 12.1.1, "Prerequisites for Configuring Oracle Unified Directory Instances"
- Section 12.1.2, "Configuring the Oracle Unified Directory Instances"
- Section 12.1.3, "Creating Access Control Lists in Non-Oracle Directories"
- Section 12.1.4, "Backing Up the Oracle Unified Directory installation"

12.1.1 Prerequisites for Configuring Oracle Unified Directory Instances

Before configuring the Oracle Unified Directory Instances on LDAPHOST1 and LDAPHOST2 ensure that the following tasks have been performed:

- Synchronize the time on the individual LDAPHOSTs nodes using Greenwich Mean Time so that there is a discrepancy of no more than 250 seconds between them.
- Install and upgrade the software on LDAPHOST1 and LDAPHOST2 as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
- Ensure that the load balancer is configured.

12.1.2 Configuring the Oracle Unified Directory Instances

Follow these steps to configure Oracle Unified Directory components in the directory tier on LDAPHOST1 and LDAPHOST2. During the configuration you will also configure Oracle Unified Directory replication servers.

This section contains the following topics:

12.1.2.1 Configuring Oracle Unified Directory on LDAPHOST1

Ensure that ports 1389, 1636, 4444, and 8989 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

```
netstat -an | grep "1389"
```

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

Remove the entries for ports 1389, 1636, 4444, and 8989 in the `/etc/services` file and restart the services or restart the computer.

Set the environment variable JAVA_HOME

Set the environment variable INSTANCE_NAME to `../../admin/oud1`. For example:

```
export INSTANCE_NAME=../../../../u02/private/oracle/config/instances/oud1
```

Note the tool creates the instance home relative to the *OUD_ORACLE_HOME*, so you must include previous directories to get the instance created in *LOCAL_CONFIG_DIR*`/instances`.

Change Directory to *OUD_ORACLE_HOME*

Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

To configure Oracle Unified Directory:

1. On the Welcome screen, click **Next**.
2. On the Server Settings screen, enter:
   - **Host Name**: The name of the host where Oracle Unified Directory is running, for example: `LDAPHOST1.example.com`
   - **LDAP Listener Port**: `1389 (LDAP_PORT)`
   - **Administration Connector Port**: `4444 (LDAP_ADMIN_PORT)`
   - **LDAP Secure Access**: Click **Configure**
   - In the Security Options page, enter:

  - **SSL Access**: Selected.
  - **Enable SSL on Port**: `1636 (LDAP_SSL_PORT)`
  - **Certificate**: Generate Self Signed Certificate OR provide details of your own certificate.
  - Click **OK**
- **Root User DN**: Enter an administrative user. For example, `cn=oudadmin`.
- **Password**: Enter the password you wish to assign to the `ouadmin` user.
- **Password (Confirm)**: Repeat the password.
- Click **Next**.

3. On the Topology Options screen:
   - Select: **This will server will be part of a replication topology**
   - Enter: **Replication Port:** `8989 (OUD_REPLICATION_PORT)`
   - Select: **Configure As Secure,** if you wish replication traffic to by encrypted.
   - There is already a server in the topology. Leave it unselected.

   Click **Next**.
4. On the Directory Data screen, enter:
   - **Directory Base DN**: `dc=example, dc=com`
   - **Directory Data**: Only create base entry

   Click **Next**.
5. On the Oracle Components Integration screen, click **Next**.
6. On the Runtime Options screen, click **Next**.
7. On the Review screen, verify that the information displayed is correct and click **Finish**.
8. On the Finished screen, click **Close**.

12.1.2.2 Validating Oracle Unified Directory on LDAPHOST1

After configuration, you can validate that Oracle Unified Directory is working by performing a simple search using the following command:

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

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

12.1.2.3 Configuring Oracle Unified Directory Instance on LDAPHOST2

Ensure that ports 1389, 1636, 4444, and 8989 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

```
netstat -an | grep "1389"
```

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

Remove the entries for ports 1389, 1636, 4444, and 8989 in the /etc/services file and restart the services or restart the computer.

Set the environment variable JAVA_HOME to *JAVA_HOME*.

Set the environment variable INSTANCE_NAME to ../../admin/oud2.

For example:

```
export INSTANCE_NAME=../../../../u02/private/oracle/config/instances/oud2
```

Note the tool creates the instance home relative to the *OUD_ORACLE_HOME*, so you must include previous directories to get the instance created in *LOCAL_CONFIG_DIR*/instances.

Change Directory to *OUD_ORACLE_HOME*

Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

1. On the Welcome screen, click **Next**.
2. On the Server Settings screen, enter the following:
   - **Host Name**: The name of the host where Oracle Unified Directory is running, for example: LDAPHOST2
   - **LDAP Listener Port**: 1389 (*LDAP_PORT*)
   - **Administration Connector Port**: 4444 (*LDAP_ADMIN_PORT*)
   - LDAP Secure Access
     - Click **Configure**
     - Select **SSL Access**
     - **Enable SSL on Port**: 1636 (*LDAP_SSL_PORT*)
     - **Certificate**: Generate Self Signed Certificate OR provide details of your own certificate.
     - Click **OK**
   - **Root User DN**: Enter an administrative user for example cn=oudadmin
   - **Password**: Enter the password you wish to assign to the ouadmin user.
   - **Password (Confirm)**: Repeat the password.
   - Click **Next**.
3. On the Topology Options screen, enter
   - **This server will be part of a replication topology**
   - **Replication Port:** 8989 (*LDAP_REPLICATION_PORT*)
   - Select **Configure As Secure,** if you wish replication traffic to by encrypted.
   - **There is already a server in the topology**: Selected.

     Enter the following:
     - **Host Name**: The name of an existing Oracle Unified Directory server host, for example: LDAPHOST1.example.com
     - **Administrator Connector Port**: 4444 (*LDAP_ADMIN_PORT*)

- **Admin User**: Name of the Oracle Unified Directory admin user on LDAPHOST1, for example: `cn=oudadmin`
- **Admin Password**: Administrator password.

Click **Next**.

If you see a certificate Not Trusted Dialogue, it is because you are using self signed certificates. Click **Accept Permanently.**

Click **Next**.

4. On The Create Global Administrator Screen Enter:
   - **Global Administrator ID:** The name of an account you want to use for managing Oracle Unified Directory replication, for example: `oudmanager`
   - **Global Administrator Password** / **Confirmation**: Enter a password for this account.

   Click **Next**.
5. On the Data Replication Screen. select `dc=example.com` and click **Next**.
6. On the Oracle Components Integration screen, click **Next**.
7. On the Runtime Options Screen, click Next.
8. On the Review Screen, check that the information displayed is correct and click **Finish**.
9. On the Finished screen, click **Close**.

12.1.2.4 Validating Oracle Unified Directory on LDAPHOST2

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

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

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

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

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

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

You then see output similar to the following example. Replication is set to enable.

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

--- Server Details ---
Host Name: slc01fnv
Administrative Users: cn=oudadmin
Installation Path: /u01/oracle/product/fmw/oud
Instance Path: /u01/oracle/admin/oud1/OUD
Version: Oracle Unified Directory 11.1.2.0.0
Java Version: 1.6.0_29
Administration Connector: Port 4444 (LDAPS)

--- Connection Handlers ---
```

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

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

12.1.2.5 Validating Oracle Unified Directory Through the Load Balancer

In addition, validate that you can access Oracle Unified Directory through the load balancer by issuing the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAP_LBR_HOST -p LDAP_LBR_PORT -D OUD_
Adminisitrator -b "" -s base "(objectclass=*)" supportedControl
```

For example:

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

12.1.2.6 Relaxing Oracle Unified Directory Object Creation Restrictions

Oracle Identity Management requires that a number of object classes be created in Oracle Unified Directory. You must perform the following step so that Oracle Unified Directory allows creation of the needed object classes.

Execute the following command on each Oracle Unified Directory instance, for example: `LDAPHOST2.example.com`

```
OUD_ORACLE_INSTANCE/OUD/dsconfig -h LDAPHOST1.example.com -p 4444 -D "cn=oudadmin"
-j ./password_file -n \
        set-global-configuration-prop \
        --set single-structural-objectclass-behavior:warn \
        --trustAll
```

12.1.2.7 Configuring a Password Policy on Oracle Unified Directory

If you want to enable Oracle Identity Manager (OIM) to lock a user account, you must configure a password policy on OUD server.

In the password policy, you must define the maximum number of failed logins the source LDAP directory server requires, to lock the account.

Use the following command to configure OUD password policy.

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig -h LDAPHOST1.example.com -p <OUD Admin SSL
port> -D <OUD Admin id> -j ./password_file -n set-password-policy-prop
--policy-name "Default Password Policy" \
--set "lockout-failure-count:10"
```

Repeat the command for each Oracle Unified Directory instance, for example: LDAPHOST2.

12.1.3 Creating Access Control Lists in Non-Oracle Directories

In the preceding sections, you seeded the Identity Store with users and artifacts for the Oracle components. If your Identity Store is not Oracle Internet Directory or Oracle Unified Directory, such as Microsoft Active Directory or Oracle Directory Server Enterprise Edition, you must set up the access control lists (ACLs) to provide appropriate privileges to the entities you created, this is true even if using Oracle Virtual Directory in front of them. This section lists the artifacts created and the privileges required for the artifacts.

- **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.
- **Access Manager Admin User**. This user is added to the OAM Administrator group, which provides permission for the administration of the Oracle Access Management Console. No LDAP schema level privileges are required, since this is just an application user.
- **Access Manager Software User**. This user 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 oimLDAP under System ID container**. Password policies are set accordingly in the container. The passwords for the users in the System ID container must be set up so that they do not expire.
- **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.
- **WebLogic Administrator**. This is the administrator of the IDM domain for Oracle Virtual Directory
- **WebLogic Administrator Group**. The WebLogic administrator is added as a member. This is the administrator group of the IDM domain for Oracle Virtual Directory.
- **Reserve container.** Permissions are provided to the Oracle Identity Manager admin group to perform read/write operations.

12.1.4 Backing Up the Oracle Unified Directory installation

After you complete the installation and configuration of each tier and verify that the install is successful, or at some other logical point, create a backup. This is a quick backup that enables you to perform an immediate restoration if you encounter problems in later steps. The backup destination is the local disk. You can discard this backup after the enterprise deployment setup is complete. At that point, you can start using the regular deployment-specific Backup and Recovery process. For more information, see *Oracle Fusion Middleware Administrator's Guide*

For information about Oracle Unified Directory database backups, see "Backing up Data" in *Oracle Unified Directory Administrator's Guide*.

To back up the installation to this point, follow these steps:

Back up the Oracle Unified Directory instances in the directory tier:

1. Shut down the instance using the commands in link to stop commands
2. 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
   ```

3. Create a backup of the Instance home on the directory tier as the root user. Type:

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

4. Start up the instance using the commands in Section 31.1.3, "Starting and Stopping Directory Services."

12.2 Configuring Oracle Internet Directory

This section describes how to create highly available Oracle Internet Directory (OID) in the enterprise deployment.

If you are using Oracle Unified Directory as your LDAP directory, you do not need Oracle Internet Directory.

This section includes the following topics:

- Section 12.2.1, "Overview of Creating an Internet Directory"
- Section 12.2.2, "Using Oracle Internet Directory in an Enterprise Deployment"
- Section 12.2.3, "Configuring the Oracle Internet Directory"

12.2.1 Overview of Creating an Internet Directory

In this chapter, you perform the following tasks:

- Configure two instances of Oracle Internet Directory by using the Oracle Identity Management 11*g* Configuration Wizard
- Validate the instances
- Tune Oracle Internet Directory

12.2.2 Using Oracle Internet Directory in an Enterprise Deployment

You use the Identity Store for storing information about users and groups. These instances can coexist on the same nodes or can exist on separate nodes. The data, however, must be stored in two separate databases. If policy information must reside in Oracle Internet Directory, you can place identity information into a different directory, such as Active Directory.

You must point `idstore.example.com` at one of the instances and `policystore.example.com` at the other.

12.2.3 Configuring the Oracle Internet Directory

This section describes how to install Oracle Internet Directory in a highly available manner. This procedure is not necessary of you are using Oracle Unified Directory as your LDAP directory.

This section contains the following topics:

- Section 12.2.3.1, "Configuring the First Oracle Internet Directory"
- Section 12.2.3.2, "Validating the OID installation on LDAPHOST1"

- Section 12.2.3.3, "Configuring Oracle Internet Directory on LDAPHOST2"
- Section 12.2.3.4, "Validating the Installation of OID on LDAPHOST2"

12.2.3.1 Configuring the First Oracle Internet Directory

Before starting the configuration disable the Oracle Internet Directory (OID) monitoring on the load balancer if it is configured. If you do not do so, then the OID administrator account becomes locked during configuration and the configuration fails.

1. Ensure that ports `3060` and `3061` are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   ```
   netstat -an | grep "3060"
   netstat -an | grep "3061"
   ```

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

2. Copy the `staticports.ini` file from the *REPOS_HOME*`/installers/idm/Disk1/stage/Response/staticports.ini` to a temporary directory on the installation media.

3. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports 3060 and 3061, as follows, uncomment the entries in the file corresponding to the entries below and set the values accordingly.

Table 12–1 OID PORTS INFORMATION

Entry	Value
Oracle Internet Directory Port No.	3060
Oracle Internet Directory (SSL) Port No.	3061

4. Start the Oracle Identity Management 11*g* Configuration Assistant by running the `config.sh` file in the following directory:

   DIR_MW_HOME`/oid/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: *LOCAL_CONFIG_DIR*`/instances/oid1`
   - Oracle Instance Name: `oid1`

   Click **Next**.

8. On the Specify Security Updates screen, choose whether to receive security updates from Oracle support and 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, and click **Next**.
11. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
    - **Connect String**: `igddb-scan.example.com:1521:igddb1^igddb-scan.example.com:1521:igdb2@oidedg.example.com`
    - **User Name**: `ODS`
    - **Password**: Enter the password for the OID schema created by RCU.
    - Click **Next**.
12. On the Configure Oracle Internet Directory screen, specify the following:
    - **Realm**: The realm where you want your company information stored, for example: `dc=example,dc=com`
    - **Administrator Password**: Password for `cn=orcladmin`
    - **Confirm Password**: Confirm administrator password.

    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. If a dialog box appears prompting you to run the `oracleRoot.sh` script. Run the `oracleRoot.sh` script, as the root user. When the following prompt appears:

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

    Enter **yes**.
15. On the Configuration Progress screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish. When it does, click **Next**.
16. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

12.2.3.2 Validating the OID installation on LDAPHOST1

To validate the installation of the Oracle Internet Directory instance on LDAPHOST1, issue these commands:

```
export ORACLE_HOME=OID_ORACLE_HOME

ORACLE_HOME/bin/ldapbind -h ldaphost1.example.com -p 3060 -D "cn=orcladmin" -q
ORACLE_HOME/bin/ldapbind -h ldaphost1.example.com -p 3061 -D "cn=orcladmin" -q -U
1
```

You are prompted for your administrator password.

> **Note:** It is important to invoke `ldapbind` from the OID Oracle Home. Many LINUX systems come with an `openldap` version of `ldapbind` which is incompatible with OID.

12.2.3.3 Configuring Oracle Internet Directory on LDAPHOST2

The schema database must be running before you perform this task.

> **Note:** Before starting the configuration, disable the OID monitoring on the load balancer if it is configured. If you do not do so, the OID administrator account becomes locked during configuration and the configuration fails.

To install Oracle Internet Directory on LDAPHOST2:

1. Ensure that ports `3060` and `3061` are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   ```
   netstat -an | grep "3060"
   netstat -an | grep "3061"
   ```

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

2. Make the temporary `staticports.ini` file created in Section 12.2.3.1 available on LDAPHOST2.

3. Start the Oracle Identity Management 11*g* Configuration Wizard by running the following command:

   DIR_MW_HOME`/oid/bin/config.sh`

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

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

   Click **Next**.

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

   Oracle Instance Location: *LOCAL_CONFIG_DIR*`/instances/oid2`

   Oracle Instance Name: `oid2`

   Click **Next**.

7. On the Specify Security Updates screen, choose whether to receive security updates from Oracle support.

   Click **Next**.

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

9. 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, and click **Next**.

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

    - Connect String: `igddb-scan.example.com:1521:igddb1^igddb-scan.example.com:1521:igdb2@oidedg.example.com`
    - **User Name:** `ODS`
    - **Password**: Enter the password for the OID schema created by RCU.

Click **Next**.

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 reuses the same schema.

Click **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 LDAPHOST1 and LDAPHOST2 is synchronized.

Click **OK** to continue.

11. On the Specify OID Admin Password screen, specify the Oracle Internet Directory administration password that you specified when creating the first OID instance.

    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. If a dialog box appears, prompting you to run the `oracleRoot.sh` script, run the `oracleRoot.sh` script, as the root user. When prompted:

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

    Enter **yes**.

14. On the Configuration Progress 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.

12.2.3.4 Validating the Installation of OID on LDAPHOST2

To validate the installation of the Oracle Internet Directory instance on LDAPHOST2, issue these commands

```
export ORACLE_HOME=OID_ORACLE_HOME

ORACLE_HOME/bin/ldapbind -h ldaphost2.example.com -p 3060 -D "cn=orcladmin" -q
ORACLE_HOME/bin/ldapbind -h ldaphost2.example.com -p 3061 -D "cn=orcladmin" -q -U
1
```

Re-enable the OID virtual host on the load balancer and check that you can access OID via the load balancer.

```
ORACLE_HOME/bin/ldapbind -h idstore.example.com -p 3060 -D "cn=orcladmin" -q
ORACLE_HOME/bin/ldapbind -h idstore.example.com -p 3061 -D "cn=orcladmin" -q -U 1
```

You are prompted for your administrator password.

Note: It is important to invoke `ldapbind` from the OID Oracle Home. Many LINUX systems come with an `openldap` version of `ldapbind`, which is incompatible with OID.

13

Preparing The Identity Store

This section describes how to prepare an existing LDAP directory manually, to use for Oracle Identity and Access Management.

> **Note:** Do not prepare the Identity Store using both manual procedure and the IDM LCM tool. If you do so, you might encounter an error or failure during the deployment.

This chapter includes the following sections:

13.1 Introduction to Preparing an Existing LDAP Directory

You may have an existing LDAP directory that you wish to use for Oracle Identity and Access Management. If you are creating a new directory, you can ignore this section, as the LCM tool does this for you. If, however, you have an existing directory you wish to use, you must first prepare it using the steps described in this chapter.

The LDAP Directory types supported are:

- Oracle Unified Directory
- Oracle Internet Directory
- Microsoft Active Directory

13.2 Creating a Configuration File

Create a property file `iam.props`, to use when preparing the Identity Store and as a basis for later integration and configuration processes. The file will have the structure described in this section. When creating the file do not include any blank lines.

The property files in this section are complete examples. Some of the parameters specified in the file will not be used until later configuration steps in the guide. It is only necessary to include the properties for the products you are going to use.

This section includes the following topics:

- Section 13.2.1, "Oracle Internet Directory Example"
- Section 13.2.2, "Oracle Unified Directory Example"
- Section 13.2.3, "Explanation of Property Values"

13.2.1 Oracle Internet Directory Example

The following is and example configuration file for Oracle Internet Directory:

```
# LDAP Properties
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 3060
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
IDSTORE_NEW_SETUP: true
# OAM Properties
IDSTORE_OAMADMINUSER: oamAdmin
IDSTORE_OAMSOFTWAREUSER: oamLDAP
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
# OIM Properties
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_OIMADMINUSER: oimLDAP
# WebLogic Properties
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: IDM Administrators
#Misc
SPLIT_DOMAIN: true
```

13.2.2 Oracle Unified Directory Example

The following is and example configuration file for Oracle Unified Directory:

```
# Common
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 1389
IDSTORE_ADMIN_PORT: 4444
IDSTORE_KEYSTORE_FILE: INSTANCE_HOME/OUD/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD: Password key
IDSTORE_BINDDN: cn=oudadmin
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_NEW_SETUP: true
POLICYSTORE_SHARES_IDSTORE: TRUE
```

```
IDSTORE_DIRECTORYTYPE: OUD
# OAM
IDSTORE_OAMADMINUSER:oamAdmin
IDSTORE_OAMSOFTWAREUSER:oamLDAP
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
# OAM and OIM
IDSTORE_SYSTEMIDBASE: cn=SystemIDs,dc=example,dc=com
# OIM
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_OIMADMINUSER: oimLDAP
# WebLogic
IDSTORE_WLSADMINUSER : weblogic_idm
IDSTORE_WLSADMINGROUP : IDM Administrators
#Misc
SPLIT_DOMAIN: true
```

13.2.3 Explanation of Property Values

This section explains the configuration file property values.

13.2.3.1 LDAP Properties

- IDSTORE_HOST and IDSTORE_PORT are, respectively, the host and port of your Identity Store directory. When preparing the Identity Store these should point to one of the LDAP instances. When configuring components such as OAM or OIM they should point to the load balancer entry point.

  For Exalogic setup, you must specify the OTD fail-over group name for this host.
- IDSTORE_DIRECTORYTYPE is the type of directory you are using. Valid values are OID, OUD
- IDSTORE_BINDDN is an administrative user in the Identity Store Directory
- IDSTORE_SEARCHBASE is the location in the directory where Users and Groups are stored.
- IDSTORE_LOGINATTRIBUTE is the LDAP attribute, which contains the users Login name.
- 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_SYSTEMIDBASE is the location of a container in the directory where system users can be placed when you do not want them in the main user container.
- IDSTORE_USERNAMEATTRIBUTE this is the name of the LDAP attribute which stores a users name.
- IDSTORE_LOGIN_ATTRIBUTE this is the name of the LDAP attribute where userids are stored.

13.2.3.2 OUD Properties

- IDSTORE_ADMIN_PORT is the administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you can leave out this parameter.

- IDSTORE_KEYSTORE_FILE is the location of the Oracle Unified Directory Keystore file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called `admin-keystore` and is located in *`OUD_INSTANCE_HOME`*`/OUD/config`. If you are not using Oracle Unified Directory, you can leave out this parameter.
- IDSTORE_KEYSTORE_PASSWORD is the encrypted password of the Oracle Unified Directory keystore. This value can be found in the file *`OUD_INSTANCE_HOME`*`/OUD/config/admin-keystore.pin`.
- IDSTORE_NEW_SETUP this parameter is used when preparing a directory for the first time.

13.2.3.3 OAM Properties

- IDSTORE_HOST and IDSTORE_PORT are, respectively, the host and port of your Identity Store directory. When preparing the Identity Store these should point to one of the LDAP instances. When configuring components such as OAM or OIM they should point to the load balancer entry point.

  For Exalogic setup, you must provide the OTD fail-over group name for this host.
- IDSTORE_OAMADMINUSER is the name of the user you want to create as your Access Manager Administrator.
- IDSTORE_OAMSOFTWAREUSER is a user that gets created in LDAP that is used when Access Manager is running to connect to the LDAP server.
- OAM11G_IDSTORE_ROLE_SECURITY_ADMIN is the name of the group, which is used to allow access to the OAM console. Only users assigned to this group will be able to access the OAM Console.
- OAM11G_SERVER_LOGIN_ATTRIBUTE this is the name of the LDAP attribute where userids are stored, this should be the same as the IDSTORE_LOGIN_ATTRIBUTE.

13.2.3.4 OIM Properties

- IDSTORE_OIMADMINGROUP Is the name of the group you want to create to hold your Oracle Identity Manager administrative users.
- IDSTORE_OIMADMINUSER is the user that Oracle Identity Manager uses to connect to the Identity store.

13.2.3.5 WebLogic Properties

- IDSTORE_WLSADMINUSER: The username to be created for logging in to the web logic domain once it is enabled by SSO.
- IDSTORE_WLSADMINGROUP: is the name of the group to which users who are allowed to log in to the WebLogic system components, such as the WLS Console and EM, belong.

13.2.3.6 Miscellaneous Properties

- SPLIT_DOMAIN is used when OAM and OIM are in different domains. This should always be set to true.

13.3 Preparing a Password File

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

You can provide these passwords in one of two ways:

- Interactively provide the passwords when prompted by idmConfigTool script.
- Create a password file that is provided an input file to the idmConfigTool script.

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

To create a password file:

Use a text editor to create a text file. You can use any file name or location, as long as it is accessible to the idmConfigTool script.

Enter the following password values in the file for example mypasswd.props:

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

13.4 Preparing an Existing LDAP Directory for LCM

If you are creating an automated deployment using the deployment wizard, you will not have access to the idmtool command described in this chapter. In such cases, if you are using Oracle Unified Directory (OUD) or Oracle Internet Directory (OID), you can choose to do one of the following:

- Let the automation tool prepare the directory for you. In this case, you do not have to follow the steps in this chapter.
- Use the standalone version of the idmConfigTool to create the objects.

  The Software Repository includes a stand alone version of the idmtool for use in these circumstances. This tool is called idmConfigTool_STA.sh and is located in the directory *LCM_HOME*/existing_directory/idmtools/bin/.

  Before using the tool, you must add the following parameter to the configuration file you created in Section 13.2, "Creating a Configuration File":

  LDIF_FILES_DIR: *LCM_HOME*/existing_directory/idmtools/templates/oid

> **Note:** You must use this path regardless of the directory type you are using, that is, Oracle Unified Directory (OUD) or Oracle Internet Directory (OID).

After you add the parameter to the configuration file, set the environment variable ORACLE_HOME to point to *LCM_HOME*/existing_directory. A sample configuration file can be found at *LCM_HOME*/existing_directory/idmtools/input_parameters.properties.

Follow the instructions in the following sections by substituting idmConfigTool_STA.sh for idmConfigTool.sh.

13.5 Preparing OID and OUD as the Identity Store

Before the LDAP directory can be used as an identity store for Oracle Access Management, it needs to be extended to include the object classes required by the product. Once it has been extended users are seeded into the directory for later use.

To prepare the Identity store perform the following steps:

- Section 13.5.1, "Configuring Oracle Internet Directory and Oracle Unified Directory"
- Section 13.5.2, "Creating Users and Groups"
- Section 13.5.3, "Granting OUD changelog Access"
- Section 13.5.4, "Updating Oracle Unified Directory ACIs for LDAP Synchronization"
- Section 13.5.5, "Creating OUD Indexes"
- Section 13.5.6, "Creating Access Control Lists in Non-Oracle Directories"

13.5.1 Configuring Oracle Internet Directory and Oracle Unified Directory

Pre-configuring the Identity Store extends the schema in Oracle Internet Directory (OID) and Oracle Unified Directory (OUD).

To do this, perform the following tasks on LDAPHOST1 if you are extending Oracle Internet Directory, or on LDAPHOST1 if you are extending Oracle Unified Directory:

Note: If your Directory is on a different host to the *IAD_ORACLE_HOME*, then the idmconfigTool.sh tool will need to be run from that host. If you have a firewall between the *IAD_ORACLE_HOME* and your directory server, you will be required to open up the LDAP ports in that firewall for the duration of this step.

If you are installing OIM only and wish to configure your directory, use *IGD_ORACLE_HOME* instead of *IAD_ORACLE_HOME*. The idmtool is the same in both the locations.

---

1. Set the environment variables - MW_HOME, JAVA_HOME, and ORACLE_HOME. Make sure you set ORACLE_HOME to *IAD_ORACLE_HOME* or *IGD_ORACLE_HOME*, and MW_HOME to *IGD_MW_HOME* or *IAD_MW_HOME*.
2. Configure the Identity Store using the command idmConfigTool from the location *IAD_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 *IAD_ORACLE_HOME*/idmtools/bin.

The syntax of the command on Linux is:

```
idmConfigTool.sh -preConfigIDStore input_file=configfile
```

For example:

```
idmConfigTool.sh -preConfigIDStore input_file=iam.props
```

When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with. This command might take some time to complete.

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.

13.5.2 Creating Users and Groups

You must seed the Identity Store with users and groups that are required by the Identity Management components.

To seed the Identity Store, perform the following tasks on OAMHOST1 or OIMHOST1:

1. Set the Environment Variables: MW_HOME, JAVA_HOME and ORACLE_HOME.

   ```
   Set ORACLE_HOME to IAM_ORACLE_HOME
   ```

   Note: Replace *IAM_ORACLE_HOME* with either *IGD_ORACLE_HOME* or *IAD_ORACLE_HOME* depending on whether the idmConfigTool is being run on OIMHOST1 or OAMHOST1.

2. Configure the Identity Store using the command idmConfigTool, at the following location:

   ```
   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 directory from which idmConfigTool is run. To ensure that each time you run the tool, it appends the same file, always run the idmConfigTool from the following directory:

   ```
   IAM_ORACLE_HOME/idmtools/bin
   ```

   The syntax of the command on Linux is:

   ```
   idmConfigTool.sh -prepareIDStore mode=MODE input_file=configfile  pwd_
   file=passwordfile
   ```

The value selected for MODE determines the type of users to be created. Possible values for MODE are: OAM, OIM, and WLS.

- In all topologies, 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. Type:

  ```
  idmConfigTool.sh -prepareIDStore mode=WLS input_file=iam.props
  ```

- If your topology includes Access Manager, you must seed the Identity Store with users that are required by Access Manager. Type:

  ```
  idmConfigTool.sh -prepareIDStore mode=OAM input_file=iam.props
  ```

- If your topology includes Oracle Identity Manager, 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. Type

  ```
  idmConfigTool.sh -prepareIDStore mode=OIM input_file=iam.props
  ```

Note: This command also creates a container in your Identity Store for reservations.

Note: When entering a password for xelsysadm ensure that it is the same at the OIM policy that is it must be at least 8 characters long, contain an Uppercase character, and a number.

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

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

13.5.3 Granting OUD changelog Access

If you are using Oracle Unified Directory, you must grant access to the changelog, by performing the following steps on LDAPHOST1 and LDAPHOST2:

1. Create a file called passwordfile which contains the password you use to connect to OUD.
2. Remove the existing change log by issuing the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop \
--remove \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)"  \
        --hostname OUD Host \
        --port OUD Admin Port \
--trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
```

```
        --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop \
--remove
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)" \
        --hostname LDAPHOST1.example.com \
        --port 4444 \
--trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
        --no-prompt
```

3. Add the new aci:

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

For example:

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

13.5.4 Updating Oracle Unified Directory ACIs for LDAP Synchronization

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

Update `OUD_ORACLE_INSTANCE/OUD/config/config.ldif` on all OUD instances with below changes:

1. Look for the following line:

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

Remove the Object Identifier (OID) `1.2.840.113556.1.4.319` from the above aci and add it to following aci as shown:

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

2. Add Object Identifiers `1.3.6.1.4.1.26027.1.5.4` and `1.3.6.1.4.1.26027.2.3.4` to the following aci as shown:

```
ds-cfg-global-aci: (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 ||
1.3.6.1.1.13.2 || 1.2.840.113556.1.4.319 || 1.2.826.0.1.3344810.2.3 ||
2.16.840.1.113730.3.4.18 || 2.16.840.1.113730.3.4.9 || 1.2.840.113556.1.4.473
|| 1.3.6.1.4.1.42.2.27.9.5.9 || 1.3.6.1.4.1.26027.1.5.4 ||
1.3.6.1.4.1.26027.2.3.4") (version 3.0; acl "Authenticated users control
access"; allow(read) userdn="ldap:///all";)
```

3. Restart the Oracle Unified Directory server on both LDAPHOSTs.

13.5.5 Creating OUD Indexes

When you ran the `idmConfigTool` to prepare an OUD identity store, it creates indexes for the data on the instance against which it is run. These indexes must be manually created on each of the OUD instances in LDAPHOST2.

To do this, run the following commands on LDAPHOST2:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a
-D "cn=oudadmin" -j password -c \
-f IAM_ORACLE_HOME/oam/server/oim-intg/ldif/ojd/schema/ojd_user_index_generic.ldif

OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a
-D "cn=oudadmin" -j  password -c \
-f IAM_ORACLE_HOME/idmtools/templates/oud/oud_indexes_extn.ldif
```

If you are performing this ready for an IDMLCM installation, use the following commands:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a
-D "cn=oudadmin" -j password -c \-f IDMLCM_HOME/existing_
directory/idmtools/templates/oid/ojd_user_index_generic.ldif

OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a
-D "cn=oudadmin" -j password -c \-f IDMLCM_HOME/existing_
directory/idmtools/templates/oud/oud_indexes_extn.ldif
```

Rebuild the Indexes

Once the indexes have been created on all of the LDAP Hosts, the indexes should be rebuilt using the commands:

1. Shutdown OUD by issuing the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/stop-ds
```

2. Execute the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/rebuild-index --rebuildAll -b "dc=example,dc=com"
```

3. Restart OUD by issuing the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/start-ds
```

4. Repeat for every LDAPHOST including the host, which the idmTool was run against, to maintain availability only stop the directory for which you are rebuilding the indexes.

13.5.6 Creating Access Control Lists in Non-Oracle Directories

In the preceding sections, you seeded the Identity Store with users and artifacts for the Oracle components. If your Identity Store is not Oracle Internet Directory or Oracle Unified Directory, such as Microsoft Active Directory or Oracle Directory Server Enterprise Edition, you must set up the access control lists (ACLs) to provide appropriate privileges to the entities you created, this is true even if using Oracle Virtual Directory in front of them. This section lists the artifacts created and the privileges required for the artifacts.

- 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.
- Access Manager Admin User. This user is added to the OAM Administrator group, which provides permission for the administration of the Oracle Access Management Console. No LDAP schema level privileges are required, since this is just an application user.
- Access Manager Software User. This user 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 oimLDAP under System ID container. Password policies are set accordingly in the container. The passwords for the users in the System ID container must be set up so that they do not expire.
- 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.
- WebLogic Administrator. This is the administrator of the IDM domain for Oracle Virtual Directory
- WebLogic Administrator Group. The WebLogic administrator is added as a member. This is the administrator group of the IDM domain for Oracle Virtual Directory.
- Reserve container. Permissions are provided to the Oracle Identity Manager admin group to perform read/write operations.

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

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

- Section 13.6.1, "Adding the Required Schemas to the Active Directory Instance"
- Section 13.6.2, "Creating the Required Containers in the Active Directory Instance"
- Section 13.6.3, "Adding Access Control Lists (ACLs) to the Containers in Active Directory"
- Section 13.6.4, "Creating Users in the Active Directory Instance"
- Section 13.6.5, "Adding User Memberships to Groups in an Active Directory Instance"

- Section 13.6.6, "Assigning Administrator Privileges to the OIMAdministrators Group"
- Section 13.6.7, "Resetting User Passwords in an Active Directory Instance"
- Section 13.6.8, "Enabling User Accounts for in an Active Directory Instance"
- Section 13.6.9, "Setting the LockoutThreshold in Active Directory"

13.6.1 Adding the Required Schemas to the Active Directory Instance

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

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

To load the schemas into the existing Active Directory instance:

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

   IAM_ORACLE_HOME/idmtools/templates/ad/

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

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

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

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

     AD_OracleSchema.ldif
     AD_OblixSchema.ldif

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

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

     AD_OracleSchema.ldif
     AD_UserSchema.ldif
     AD_oam_pwd_schema_add.ldif

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

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

13.6.2 Creating the Required Containers in the Active Directory Instance

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

To create the required containers:

1. Create a new LDIF file that can be used to create the containers required for your topology.
   - If you are planning to deploy an OAM and OMSS topology, create a `.ldif` file as shown in Example 13–1.
   - If you are planning to deploy an integrated OIM, OAM, and OMSS topology, create a `.ldif` file as shown in Example 13–2.

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

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

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

Example 13–1 Sample LDIF File Used to Create Containers for an OAM and OMSS Deployment

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

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

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

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

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

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

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

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

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

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

Example 13–2 Sample LDIF File to Create Containers for an Integrated OIM, OAM, and OMSS Topology

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

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

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

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

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

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

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

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

dn: cn=IDM Administrators,cn=Groups,dc=example,dc=com
```

```
changetype: add
cn: IDM Administrators
sAMAccountName: IDM Administrators
objectclass: group

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

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

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

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

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

Follow the instructions in the following article on the Microsoft TechNet Web site to add the ACLs listed in Example 13–3:

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

Example 13–3 List of ACLs for the Required Active Directory Containers

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

13.6.4 Creating Users in the Active Directory Instance

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

1. Create a new LDIF file that can be used to create the users required for your topology:
   - If you are planning to deploy an OAM and OMSS topology, create a `.ldif` file as shown in Example 13–4.
   - If you are planning to deploy an integrated OIM, OAM, and OMSS topology, then create a `.ldif` file as shown in Example 13–5.

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

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

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

Example 13–4 Sample LDIF File for Adding Users to the Active Directory Instance for an OAM and OMSS Topology

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

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

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

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

Example 13–5 Sample LDIF File to Create Users in an Active Directory Instance for an Integrated OIM, OAM, and OMSS Topology

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

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

```
cn: xelsysadm
userPrincipalName: xelsysadm

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

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

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

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

13.6.5 Adding User Memberships to Groups in an Active Directory Instance

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

- For an OAM and OMSS topology, the groups and their associated users are shown in Section 13.6.5.1.
- For an integrated OIM, OAM, and OMSS deployment, the groups and their associated users are shown in Section 13.6.5.2.

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

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

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

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

- `cn=IDM Administrators,cn=Groups,dc=example,dc=com`

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

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

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

- cn=IDM Administrators,cn=Groups,dc=example,dc=com
  - cn=oamadministrators,cn=groups,dc=example,dc=com
  - cn=weblogic_idm,cn=users,dc=example,dc=com
- cn=OAMAdministrators,cn=Groups,dc=example,dc=com
  - cn=oamadmin,cn=users,dc=example,dc=com
- cn=OIMAdministrators,cn=Groups,dc=example,dc=com
  - cn=oimldap,cn=systemids,dc=example,dc=com
- cn=orclFAGroupReadPrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=orclFAOAMUserWritePrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=orclFAUserReadPrivilegeGroup,cn=Groups,dc=example,dc=com
  - cn=oamldap,cn=systemids,dc=example,dc=com
- cn=BIReportAdministrator,cn=Groups,dc=example,dc=com
  - cn=xelsysadm,cn=Users,dc=example,dc=com

13.6.6 Assigning Administrator Privileges to the OIMAdministrators Group

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

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

5. Click **OK** to close the Select Groups dialog box.
6. Click **Apply** to apply your changes.

13.6.7 Resetting User Passwords in an Active Directory Instance

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

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

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

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

13.6.8 Enabling User Accounts for in an Active Directory Instance

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

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

13.6.9 Setting the LockoutThreshold in Active Directory

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

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

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

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

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

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

14 Configuring the Oracle Web Tier

This chapter describes how to configure the Web Tier for an Oracle Identity and Access Manager enterprise deployment. There are two possible Web tier configurations, Oracle HTTP Server, or Oracle Traffic Director.

This chapter contains the following sections:

- Configuring Oracle HTTP Server
- Configuring Oracle Traffic Director
- Backing up the Web Tier Configuration

14.1 Configuring Oracle HTTP Server

This section describes how to associate the Oracle HTTP Server with the WebLogic Server domain. Once the Oracle HTTP Server is associated with the WebLogic Server, you can monitor it using the Oracle Fusion Middleware Console.

You then configure the load balancer to route all HTTP requests to WEBHOST1 and WEBHOST2.

The last section describes how to define the Oracle HTTP Server directives to route requests to the load balancer virtual hosts.

This section contains the following topics:

- Section 14.1.1, "Running the Configuration Wizard to Configure the HTTP Server"
- Section 14.1.2, "Configuring Virtual Hosts"

14.1.1 Running the Configuration Wizard to Configure the HTTP Server

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

Oracle HTTP Server is installed by default on port 7777. 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 configuring Oracle HTTP Server. You must free the port if it is in use.

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

Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the `staticports.ini` file located in the following directory:

```
stage/Response
```

Copy it to a file called ohs_ports.ini. Delete all entries in ohs_ports.ini except for OHS PORT and OPMN Local Port. Change the values of those ports to 7777 and 6700, respectively. Or different ports if you prefer to use the standard ones.

> **Note:** If the port names in the file are slightly different from OHS PORT and OPMN Local Port, use the names in the file.

To configure the Oracle Web tier, do the following:

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

   ```
   cd OHS_ORACLE_HOME/bin
   ```

2. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

   Ensure that **Associate Selected Components with WebLogic Domain** and **Oracle Web Cache** are **NOT** selected.

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

   Enter the following values for WEBHOST1:

   - Instance Home Location: *LOCAL_CONFIG_DIR*/instances/ohs1
   - Instance Name: ohs1
   - OHS Component Name: ohs1

   Click **Next**.
4. On the Configure Ports screen, you use the ohs_ports.ini file you created above to specify the ports to be used. This enables you to bypass automatic port configuration.
   a. Select **Specify Ports using a Configuration File**.
   b. In the file name field specify the absolute path to the ohs_ports.ini file. You can use the **Browse** button to locate the file, and then click **Open**.
   c. Click **Save**, then click **Next**.
5. On the Specify Security Updates screen, choose whether to skip updates, or enter your Oracle Support Details to be notified of security updates.

   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**.
7. On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.
8. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

9. Repeat for WEBHOST2 using Instance/component name `ohs2`.

Validating the Configuration

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

```
http://WEBHOST1.example.com:7777/
http://WEBHOST2.example.com:7777/
```

14.1.2 Configuring Virtual Hosts

To configure the virtual hosts complete the following tasks as described in this section.

- Section 14.1.2.1, "Configuring Virtual Hosts"
- Section 14.1.2.2, "Configuring Oracle HTTP Server to Run as Software Owner"
- Section 14.1.2.3, "Updating Oracle HTTP Server Runtime Parameters"
- Section 14.1.2.4, "Validating the Configuration"
- Section 14.1.2.5, "Backing Up the Web Tier Configuration"

14.1.2.1 Configuring Virtual Hosts

This section includes all of the Web tier configurations for all products covered in the Enterprise Deployment Blueprint. If you are only configuring a subset of the topology then include only those entries suitable for your topology.

Create an OHS configuration file for each virtual host within the deployment, in the following location

OHS_ORACLE_INSTANCE/config/OHS/<component>/moduleconf.

> **Note:** The following sections show all entries for all components. If you are only deploying a subset of the components you only need to include those entries. `NameVirtualHost` is only required in the first file that is read. You can either put this entry into the first file name alphabetically, or directly into the `httpd.conf` file.

These files should appear as following

iadadmin_vh.conf

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName http://iadadmin.example.com:80
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   UseCanonicalName On
   ServerAdmin you@your.address
#Weblogic related entries
# Admin Server and EM

<Location /console>
```

```
   WLSRequest ON
   WebLogicHost iadadminvhn.example.com
   WeblogicPort 7001
</Location>

<Location /consolehelp>
   WLSRequest ON
   WebLogicHost iadadminvhn.example.com
   WeblogicPort 7001
</Location>

<Location /em>
   WLSRequest ON
   WebLogicHost iadadminvhn.example.com
   WeblogicPort 7001
</Location>

<Location /oamconsole>
   WLSRequest ON
    WebLogicHost iadadminvhn.example.com
    WeblogicPort 7001
</Location>

<Location /apm>
   WLSRequest ON
   WebLogicHost iadadminvhn.example.com
   WeblogicPort 7001
</Location>

<Location /access>
   WLSRequest ON
   WebLogicCluster oamhost1.example.com:14150,oamhost2.example.com:14150
   WLCookieName OAMJSESSIONID
</Location>

<Location /gms-rest>
    WLSRequest ON
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>

<Location /msm-mgmt>
    WLSRequest ON
    WLCookieName OAMJSESSIONID
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>
</VirtualHost>
```

igdadmin_vh.conf (if using a split domain topology)

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName http://igdadmin.example.com:80
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   UseCanonicalName On
```

```
   ServerAdmin you@your.address
   # Weblogic Admin Server and EM

   <Location /console>
      WLSRequest ON
      WebLogicHost igdadminvhn.example.com
      WeblogicPort 7101
   </Location>

    <Location /consolehelp>
      WLSRequest ON
      WebLogicHost igdadminvhn.example.com
      WeblogicPort 7101
   </Location>

  <Location /em>
      WLSRequest ON
      WebLogicHost igdadminvhn.example.com
      WeblogicPort 7101
   </Location>

##################################################
## Entries Required by Oracle Entitlements Server
##################################################
   # APM
<Location /apm>
   WLSRequest ON
   WebLogicHost igdadminvhn.example.com
   WeblogicPort 7101
</Location>

##############################################
## Entries Required by Oracle Identity Manager
##############################################
<Location /oim>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

   <Location /sysadmin>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# OIM self service console
```

```
   <Location /identity>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Nexaweb WebApp - used for workflow designer and DM
   <Location /Nexaweb>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Scheduler webservice URL
   <Location /SchedulerService-web>
      WLSRequest ON
      WLCookieName    oimjsessionid
      WebLogicCluster
 oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Oracle BIP console
   <Location /xmlpserver>
      WLSRequest ON
      WLCookieName   JSESSIONID
      WebLogicCluster oimhost1vhn3.example.com:9704,oimhost2vhn3.example.com:9704
      WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
</VirtualHost>
```

login_vh.conf

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName https://login.example.com:443
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end
_url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
 [R]
   UseCanonicalName On
   ServerAdmin you@your.address

   #OAM Entries
   <Location /oam>
       WLSRequest ON
       WLProxySSL ON
       WLProxySSLPassThrough ON
       WLCookieName OAMJSESSIONID
       WebLogicCluster oamhost1.example.com:14100,oamhost2.example.com:14100
   </Location>

   <Location /oamfed>
       WLSRequest ON
       WebLogicCluster oamhost1.example.com:14100,oamhost2.example.com:14100
```

```
       WLCookieName OAMJSESSIONID
      WLProxySSL ON
      WLProxySSLPassThrough ON
  </Location>

  <Location /ms_oauth >
       WLSRequest ON
       WebLogicCluster oamhost1.example.com:14100,oamhost2.example.com:14100
       WLCookieName OAMJSESSIONID
       WLProxySSL ON
    WLProxySSLPassThrough ON
  </Location>
</VirtualHost>
```

prov_vh.conf

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName https://prov.example.com:443
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end
_url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   UseCanonicalName On
   ServerAdmin you@your.address
  <Location /identity>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    WLProxySSL ON
    WLProxySSLPassThrough ON
    </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    WLProxySSL ON
    WLProxySSLPassThrough ON
  </Location>

<Location /HTTPClnt>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    WLProxySSL ON
    WLProxySSLPassThrough ON
  </Location>

# Requests webservice URL
  <Location /reqsvc>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLProxySSL ON
```

```
    WLProxySSLPassThrough ON
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>
</VirtualHost>
```

iadinternal_vh.conf

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName http://iadinternal.example.com:7777
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end
_url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
 [R]
   UseCanonicalName On
   ServerAdmin you@your.address
#MSM Entries

<Location /msm>
    WLSRequest ON
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
           WLCookieName OAMJSESSIONID
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
   </Location>

# MSM runtime services for MAM
<Location /ecp>
    WLSRequest ON
           WLCookieName OAMJSESSIONID
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>

# Mobile File manager
<Location /mfm>
    WLSRequest ON
           WLCookieName OAMJSESSIONID
              WebLogicCluster
 oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>

# MSAS management services
<Location /gms-rest>
    WLSRequest ON
    WLCookieName OAMJSESSIONID
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>

# MSM management rest services
<Location /msm-mgmt>
    WLSRequest ON
    WLCookieName OAMJSESSIONID
    WebLogicCluster oamhost1.example.com:14180,oamhost2.example.com:14180
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/msm_component.log"
</Location>
</VirtualHost>
```

igdinternal_vh.conf

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName http://igdinternal.example.com:7777
   RewriteEngine On
   RewriteOptions inherit
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   UseCanonicalName On
   ServerAdmin you@your.address

################################################
## Entries Required by Oracle Identity Manager
################################################
#SOA Callback webservice for SOD - Provide the SOA Managed Server Ports

 <Location /sodcheck>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn2.example.com:8001,oimhost2vhn2.example.com:8001
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/soa_component.log"
  </Location>

# OIM, role-sod profile
  <Location /role-sod>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    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>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/soa_component.log"
  </Location>

# used for FA Callback service.
  <Location /callbackResponseService>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

# spml xsd profile
  <Location /spml-xsd>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

# OIM, spml dsml profile
  <Location /spmlws>
```

```
    WLSRequest ON
    PathTrim /weblogic
    WLCookieName oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

  <Location /reqsvc>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/soa_component.log"
  </Location>

  <Location /integration>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn2.example.com:8001,oimhost2vhn2.example.com:8001
  </Location>

 # SOA Infra
  <Location /soa-infra>
    WLSRequest ON
    WLCookieName oimjsessionid
    WebLogicCluster OIMHOST1VHN2.example.com:8001,OIMHOST2VHN2.example.com:8001
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/component/oim_
component.log"
  </Location>

# UMS Email Support
  <Location /ucs>
    WLSRequest ON
    WLCookieName oimjsessionid
    WebLogicCluster OIMHOST1VHN2.example.com:8001,OIMHOST2VHN2.example.com:8001
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/component/oim_
component.log"
  </Location>

  <Location /provisioning-callback>
    WLSRequest ON
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

<Location /CertificationCallbackService>
   WLSRequest ON
   WLCookieName    oimjsessionid
   WebLogicCluster oimhost1vhn1.example.com:14000,oimhost2vhn1.example.com:14000
   WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
</VirtualHost>
```

Restart OHS on WEBHOST1 and WEBHOST2 using the procedures in Section 31.1.3, "Starting and Stopping Directory Services."

14.1.2.2 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 *`OHS_ORACLE_INSTANCE`*`/config/OHS/`*`component_name`*.

Find the section in `httpd.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>
```

14.1.2.3 Updating Oracle HTTP Server Runtime Parameters

By default, the Oracle HTTP Server contains parameter values that are suitable for most applications. These values, however, must be adjusted in IDM Deployments.

Proceed as follows:

Edit the file `httpd.conf`, which is located in:

`OHS_ORACLE_INSTANCE``/config/OHS/component_name`

Find the entry that looks like this:

```
<IfModule mpm_worker_module>
```

Update the values in this section as follows:

```
<IfModule mpm_worker_module>
  ServerLimit       20
  StartServers      10
  MaxClients      1000
  MinSpareThreads  200
  MaxSpareThreads  800
  ThreadsPerChild   50
  ThreadLimit       50
  MaxRequestsPerChild  1000
  AcceptMutex fcntl
```

```
  LockFile "${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_
NAME}/http_lock"
</IfModule>
```

Save the file.

Restart the OHS servers using the following commands:

```
ORACLE_INSTANCE/bin/opmnctl stopall
ORACLE_INSTANCE/bin/opmnctl startall
```

14.1.2.4 Validating the Configuration

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

```
http://WEBHOST1.example.com:7777/

http://WEBHOST2.example.com:7777/

https://prov.example.com

https://login.example.com

http://iadadmin.example.com

http://igdadmin.example.com

http://igdinternal.example.com:7777

http://iadinternal.com:7777
```

14.1.2.5 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.

14.2 Configuring Oracle Traffic Director

Oracle Traffic Director is a software load balancer for load balancing HTTP/S and TCP traffic to servers in the backend. These backend servers, which are referred to as origin servers within Oracle Traffic Director, can be application servers, web servers, or LDAP servers.

Installing and configuring Oracle Traffic Director for an enterprise deployment involves performing the steps shown in Table 14–1.

Table 14–1 Overview of Installing and Configuring Oracle Traffic Director for an Enterprise Deployment

Task	Description	More Information
Review Oracle Traffic Director prerequisites.	For example, be sure that you have set up the required virtual IP addresses, that the user account has root permission on the storage appliance, and that you have already created the initial Oracle WebLogic Server domain for the Oracle Identity Management topology.	"Prerequisites" in the *Oracle Traffic Director Installation Guide*
Install the Oracle Traffic Director software.	You install the software using the directories and mount points you created in Section 7.5.5, "Recommended Directory Locations."	Section 11.2.2, "Installing Oracle Traffic Director"
Create and start an Oracle Traffic Director Administration Server.	The Oracle Traffic Director administration server hosts the administration console and command-line interface, through which you can create Oracle Traffic Director configurations, deploy them as instances on administration nodes, and manage the instances.	Section 14.2.1, "Creating and Starting the Traffic Director Administration Server"
Verify the installation.	Be sure that the installation was successful before you continue configuring the environment.	"Verifying the Installation" in the *Oracle Traffic Director Installation Guide*
Register WEBHOST2 as administration node.	This ensures that Oracle Traffic Director is up and running on both WEBHOST1 and WEBHOST2.	Section 14.2.2, "Registering WEBHOST2 with the Administration Node"
Create a configuration	The configuration should route requests from the Oracle Traffic Director instances to the managed servers in the Oracle WebLogic Server domain. The configuration should also define the required origin-server pools to which requests should be routed.	Section 14.2.3, "Creating a Configuration"
Start the Oracle Traffic Director instances	Start the instances on WEBHOST1 and WEBHOST2, based on the configuration you created earlier in this procedure.	Section 14.2.4, "Starting, Stopping, and Restarting Oracle Traffic Director"
Define the virtual servers.	Define the virtual servers required for accessing the various management tools and login screens for the topology.	Section 14.2.5, "Defining the Required Oracle Traffic Director Virtual Servers for an Enterprise Deployment"
Create Routes	Adding routes allows a virtual server to direct requests to different server pools depending on what is contained within the URI.	Section 14.2.6, "Creating Routes"

Table 14–1 (Cont.) Overview of Installing and Configuring Oracle Traffic Director for an Enterprise

Task	Description	More Information
Enable SSL Passthrough for login.example.com	Perform extra configuration steps to ensure that any application redirects occur correctly.	Section 14.2.7, "Enabling SSL Passthrough"
Deploy and test the configuration.	Deploy the configuration and test the virtual server URLs to be sure you have configured the Oracle Traffic Director instances successfully.	Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses"
Create an active-passive failover group.	Create a failover group to ensure that requests will continue to be served if WEBHOST1 or WEBHOST2 become unavailable.	Section 14.2.10, "Creating a Failover Group for Virtual Hosts"

This section contains the following topics:

- Section 14.2.1, "Creating and Starting the Traffic Director Administration Server"
- Section 14.2.2, "Registering WEBHOST2 with the Administration Node"
- Section 14.2.3, "Creating a Configuration"
- Section 14.2.4, "Starting, Stopping, and Restarting Oracle Traffic Director"
- Section 14.2.5, "Defining the Required Oracle Traffic Director Virtual Servers for an Enterprise Deployment"
- Section 14.2.6, "Creating Routes"
- Section 14.2.7, "Enabling SSL Passthrough"
- Section 14.2.8, "Workaround for Issues caused by TMPWATCH cleanup"
- Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses"
- Section 14.2.10, "Creating a Failover Group for Virtual Hosts"

14.2.1 Creating and Starting the Traffic Director Administration Server

After you install Oracle Traffic Director on WEBHOST1 and WEBHOST2, you can then create an Oracle Traffic Director administration server.

You can configure Oracle Traffic Director to run either as root or as a non-privileged user. Oracle recommends configuring it to run as root although instructions for both are included in this chapter. Running Oracle Traffic Director as root allows all administrative tasks such as starting and stopping instances to be run from the Oracle Traffic Director administration console.

If you decide not to configure Oracle Traffic Director to run as root, additional steps are required outside of the Oracle Traffic Director console using the root account. This is because failover groups (discussed later) require the running of processes to which only root has access.

For more information, see "Managing the Administration Server" in the *Oracle Traffic Director Administrator's Guide*

To create the Oracle Traffic Director administration server on WEBHOST1 run the **`tadm`** command from the *OTD_ORACLE_HOME*`/bin` directory, as follows:

1. On WEBHOST1 enter the following command:

```
OTD_ORACLE_HOME/bin/tadm configure-server --port=OTD_ADMIN_PORT \
--user=otdadmin --instance-home=OTD_ORACLE_INSTANCE --host=OTDADMINVHN
--server-user=root
```

Where:

- *OTD_ORACLE_HOME* the Oracle Home location you entered in the Oracle Traffic Director installer.
- *OTD_ORACLE_INSTANCE* is the recommended value listed in Table 7–4, " Private Storage Directories - Distributed Topology".
- `OTDADMINVHN` is the virtual host name to be used for the Oracle Traffic Director administration server and console.

For example:

```
OTD_ORACLE_HOME/web/bin/tadm configure-server --port=8800 --user=otdadmin \
--instance-home=/u02/private/oracle/config/instances/otd1
--host=OTDADMINVHN.example.com
```

Note: If you want to run Oracle Traffic Director as the root user, which is necessary if you want Oracle Traffic Director to work using ports <1024, you must add the following additional parameter to the command:

```
--server-user=root
```

---

2. Enter the administrator password.

   You will later use this password to log in to the Oracle Traffic Director administration console.

   A prompt to re-enter the administrator password is displayed, as follows:

   ```
   Please enter admin-user-password again>
   ```

3. Confirm the administrator password by entering it again.

   An Administration Server instance of Oracle Traffic Director is created and deployed on the local host in a directory named `admin-server` within the *OTD_ORACLE_INSTANCE* directory that you specified in step 1.

4. Start the Administration Server by running the following command on WEBHOST1:

   ```
   WEB_INSTANCE_HOME/admin-server/bin/startserv
   ```

   If you want the server to run as `root`, start it as `root`.

5. Log in to the Administration Server using the following URL:

   ```
   https://OTDADMINVHN:8800
   ```

   where 8800 is *OTD_ADMIN_PORT*.

   Use the password provided above and verify that you can see the Oracle Traffic Director main page.

14.2.2 Registering WEBHOST2 with the Administration Node

This section assumes you have installed Oracle Traffic Director, started the Administration Server, and verified the installation.

WEBHOST1 and WEBHOST2 have IP over InfiniBand (IPoIB) addresses. For example, 192.168.10.5 and 192.168.10.6.

You can now register WEBHOST2 with the Oracle Traffic Director Administration Server using the **tadm** command from the *OTD_ORACLE_HOME*/bin directory, as follows:

1. On the WEBHOST2, run the configure-server command to register the host with the remote Administration Server as an administration node.

```
./tadm configure-server --user=otdadmin --port=OTD_ADMIN_PORT
--host=OTDADMINVHN \
--admin-node --node-port=OTD_NODE_PORT --instance-home=OTD_ORACLE_INSTANCE
--node-host=WEBHOST2 --server-user=root
```

   Where:

   - *OTD_ORACLE_HOME* is the path to the Oracle Traffic Director Oracle home on WEBHOST2.
   - *WEB_INSTANCE_HOME* is the recommended directory path listed in Table 7–4, " Private Storage Directories - Distributed Topology"
   - *node-host* is the name of the machine that this instance is running on (IAMHOST1, IAMHOST2, or WEBHOST2).

   For example:

```
./tadm configure-server --user=otdadmin --port=8800 --host=OTDADMINVHN
--admin-node \
--node-port=8900 --instance-home=/u02/private/oracle/config/instances/otd2
--node-host=WEBHOST2
```

   Note: If you want to run Oracle Traffic Director as the root user, which is necessary if you want Oracle Traffic Director to work using ports <1024, you must add the following additional parameter to the command:

```
--server-user=root
```

   For more information, see "configure-server" in the *Oracle Traffic Director Command-Line Reference* or use the configure-server --help command to see an explanation of the command line options.

   The following prompt appears after you run configure-server command:

```
This command creates an Administration Node and register it with the following
remote Administration Server: https://WEBHOST1.example.com

Enter admin-user password>
```

2. Enter the admin-user password for the Oracle Traffic Director Administration Server.

The `configure-server` command attempts to connect to the remote administration server by using the specified administration server host, port, user, and password. The Administration Server on WEBHOST1 must be up and running.

If this is the first time that the host on which you are creating the administration node is attempting to connect to the administration server, the server certificate of the administration server is displayed.

3. Enter `y` to trust the certificate.

   The following message is displayed:

   ```
   OTD-70215 The administration node has been configured successfully.
   The node can be started by executing:
   OTD_ORACLE_INSTANCE/admin-server/bin/startserv
   ```

4. Start the Oracle Traffic Director Server by running the following command on WEBHOST2:

   ```
   WEB_INSTANCE_HOME/admin-server/bin/startserv
   ```

   If you want the server to run as `root`, start it as `root`.

After you start the administration node, you can create instances of Oracle Traffic Director configurations on the administration node. Note that on each administration node, you can create only one instance of a configuration.

14.2.3 Creating a Configuration

The next step in installing and configuring Oracle Traffic Director for an enterprise deployment is to create a configuration that will route requests to a server pool that consists of the managed servers in your Oracle WebLogic Server domain.

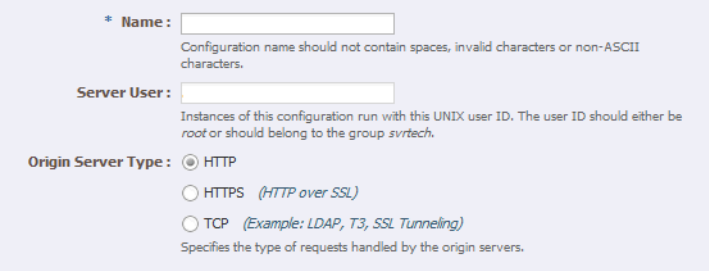
When creating a new configuration, you are required to provide the host and port information for the origin server, which in turn automatically creates (and names) an origin-server pool called **origin-server-pool-1**. This is the default origin-server pool and this pool can be found when you click the Server Pools option in the administration console. You cannot rename the default origin-server pool.

To create a configuration named IAM by using the administration console:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs."
2. In the Common Tasks pane, click **New Configuration**.

   The New Configuration wizard starts.

Figure 14–1 New Configuration Wizard



3. In the Step 1 Configuration Information screen, enter the following information:

- **Name:** `login.example.com`
- **Server User:** `oracle` (or `root`, if you want the server instances to run as `root`).
- **Origin Server Type**: Make sure **HTTP** is selected.

Click **Next**.

4. On the Configure Listener Information Screen, set the listener port to the `WEB_HTTP_PORT`. For example: `7777`.

> **Note:** If you are deploying Oracle Identity and Access Management using the IDM LCM tool, the listener port should be set to a temporary value such as `6666`. This is because, the automation tool install Oracle HTTP server on the `WEB_HTTP_PORT`. Once the IDMLCM installation is completed, you will disable the Oracle HTTP servers and update the OTD listen port to the WEB_HTTP_PORT value. This ensures that, when IDMLCM performs its inter-application writing, it does so using the `WEB_HTTP_PORT`. When the Oracle HTTP servers are disabled, OTD will then assume the role of the Web Server.

Accept the other default values and click **Next.**

5. In the Step 3 Server Pool Information screen:
   a. In the **Origin Servers: Host:** field, enter *OAMHOST1*`.example.com`, the port `14100` (*`OAM_PORT`*), and click **Add Server**.
   b. Enter *OAMHOST2*`.example.com` and port `14100`, click **Add Server** and click **Next**.
6. In the Step 4 Deployment Information screen, select the **Administration Server** and *WEBHOST2* and click **Next**.

   The Review screen appears.
7. Review the information and click **Create Configuration**.

   The Results screen appears.

   After the configuration is created, the Results screen of the New Configuration wizard displays a message confirming successful creation of the configuration. If you chose to create instances of the configuration, then a message confirming successful creation of the instances is also displayed.
8. Click **Close** on the Results screen.

   In the New Configuration wizard, if you chose not to create an instance of the configuration, the message **Undeployed Configuration** is displayed, indicating that the configuration that you just created is yet to be deployed.

14.2.4 Starting, Stopping, and Restarting Oracle Traffic Director

To start and stop Oracle Traffic Director instances see Section 31.1.7.2, "Starting the Oracle Traffic Director Instances"

14.2.5 Defining the Required Oracle Traffic Director Virtual Servers for an Enterprise Deployment

Create and configure the virtual servers for the Oracle Traffic Director configuration. In this section you create the following Oracle Traffic Director virtual servers for your

Oracle Identity and Access Management deployment. If External Oracle HTTP Servers are being used then several of these virtual servers should not be enabled on the Oracle Traffic Director.

Table 14–2 Defining OTD Virtual Servers

Virtual Server	Purpose	Creating the Virtual Server	Required with OHS
login.example.com	Acts as the access point for all HTTP traffic that gets directed to the single sign on services.	This virtual server is created through administration console in Section 14.2.5.2, "Creating Virtual Servers.".	No
prov.example.com	Acts as the access point for all HTTP traffic that gets directed to the provisioning applications.	The virtual server is created through the administration console in Section 14.2.5.2, "Creating Virtual Servers."	No
iadadmin.example.com	Acts as the access point for all internal HTTP traffic that gets directed to the IAMAccessDomain administration services.	This virtual server is created through administration console in Section 14.2.5.2, "Creating Virtual Servers.".	No
igdadmin.example.com	Acts as the access point for all internal HTTP traffic that gets directed to the IAMGovernanceDomain administration services.	This virtual server is created through administration console in Section 14.2.5.2, "Creating Virtual Servers."	No
iadinternal.example.com	Acts as the access point for all internal HTTP traffic requests that get directed to Mobile Security Manager (MSM).	The virtual server is created through the administration console in Section 14.2.5.2, "Creating Virtual Servers.".	No
igdinternal.example.com	Acts as the access point for all internal HTTP traffic requests that get directed to OIM and SOA.	This virtual server is created through administration console in Section 14.2.5.2, "Creating Virtual Servers.".	Yes
idstore.example.com	Acts as the access point for all Identity Store LDAP traffic.	This virtual server is created when you configure the TCP Proxy for OUD in Section 14.2.5.3, "Creating a TCP Proxy and Listener for idstore.example.com.".	Yes

To create and configure virtual servers using the administration console complete the steps in the following sections:

- Section 14.2.5.1, "Creating OTD Origin Server Pools"
- Section 14.2.5.2, "Creating Virtual Servers"
- Section 14.2.5.3, "Creating a TCP Proxy and Listener for idstore.example.com"

14.2.5.1 Creating OTD Origin Server Pools

A server pool is a group of one or more virtualization hosts with the same processor architecture that have access to the same virtual and physical networks, and storage resources. Server pools provide load balancing, high availability capabilities, and sharing of some resources for all members of the pool.

In this section, create the Oracle Traffic Director origin-server pools listed in Table 14–3.

Table 14–3 Origin-Server Pools and Origin Servers for Physical Exalogic

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.example.com	7001 (*IAD_WLS_PORT*)
igdadmin-pool	HTTP	IGDADMINVHN.example.com	7101 (*IGD_WLS_PORT*)
ldap-pool	TCP	IAMHOST1.example.com, IAMHOST2.example.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHN1.example.com, OIMHOST2VHN1.example.com	14000 (*OIM_PORT*)
ama-pool	HTTP	IAMHOST1.example.com, IAMHOST2.example.com	14150 (*AMA_PORT*)
msm-pool	HTTP	IAMHOST1.example.com, IAMHOST2.example.com	14180 (*MSM_PORT*)
origin-server-pool-1	HTTP	IAMHOST1.example.com, IAMHOST2.example.com	14100 (*OAM_PORT*)
soa-pool	HTTP	OIMHOST1VHN2.example.com, OIMHOST2VHN2.example.com	8001 (*SOA_PORT*)
bi-pool	HTTP	OIMHOST1VHN3.example.com, OIMHOST2VHN3.example.com	9704 (*BI_PORT*)

Table 14–4 Origin-Server Pools and Origin Servers for Virtual Exalogic

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.example.com	7001 (*IAD_WLS_PORT*)
igdadmin-pool	HTTP	IGDADMINVHN.example.com	7101 (*IGD_WLS_PORT*)
ldap-pool	TCP	LDAPHOST1.example.com, LDAPHOST2.example.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHN1.example.com, OIMHOST2VHN1.example.com	14000 (*OIM_PORT*)
origin-server-pool-1	HTTP	OAMHOST1.example.com, OAMHOST2.example.com	14100 (*OAM_PORT*)
soa-pool	HTTP	OIMHOST1VHN2.example.com, OIMHOST2VHN2.example.com	8001 (*SOA_PORT*)
bi-pool	HTTP	OIMHOST1VHN3.example.com, OIMHOST2VHN3.example.com	9704 (*BI_PORT*)
ama-pool	HTTP	OAMHOST1.example.com,OAMHOST2.example.com	14150 (*IAMADM_PORT*)
msm-pool	HTTP	OAMHOST1.example.com,OAMHOST2.example.com	14180 (*IAMADM_PORT*)

Table 14–5 Origin-Server Pools and Origin Servers for External OHS Servers

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.example.com	7001 (*IAD_WLS_PORT*)
igdadmin-pool	HTTP	IGDADMINVHN.example.com	7101 (*IGD_WLS_PORT*)
ldap-pool	TCP	IAMHOST1-EXT.example.com, IAMHOST2-EXT.example.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHN2-EXT.example.com OIMHOST2VHN2-EXT.example.com	14000 (*OIM_PORT*)
bi-pool	HTTP	OIMHOST1VHN3-EXT.example.com, OIMHOST2VHN3-EXT.example.com	9704 (*BI_PORT*)
origin-server-pool-1	HTTP	IAMHOST1-EXT.example.com, IAMHOST2-EXT.example.com	14100 (*OAM_PORT*)
soa-pool	HTTP	OIMHOST1VHN2.example.com, OIMHOST2VHN2.example.com	8001 (*SOA_PORT*)
ama-pool	HTTP	IAMHOST1-EXT.example.com, IAMHOST2-EXT.example.com	14150 (*AMA*)
msm-pool	HTTP	IAMHOST1-EXT.example.com, IAMHOST2-EXT.example.com	14180 (*IAMMSM_PORT*)

Note: The `origin-server-pool-1` is created automatically for you when you created the configuration.

To create an origin-server pool:

1. Log in to the Administration Console using the following URL:

   `https://OTDADMINVHN:`*`OTD_ADMIN_PORT`*

   where *OTD_ADMIN_PORT* is defined in Section 8.1, "Summary of Virtual IP Addresses Required."

2. Click the **Configurations** button that is situated at the upper left corner of the page.

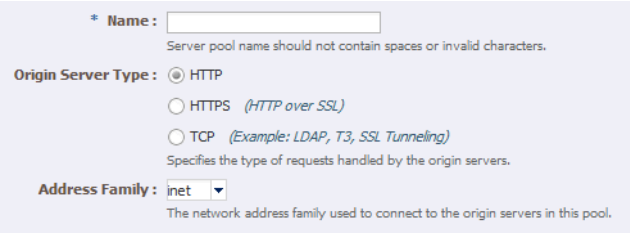
   A list of the available configurations is displayed.

3. Select the configuration for which you want to create a server pool. For example, `login.example.com`.

4. In the **Common Tasks** pane, click **New Server Pool**.

   The New Origin-Server Pool wizard starts.

Figure 14–2 New Origin-Server Pool Wizard



5. Enter the following information in the Server Pool Information screen:
   - **Name:** Name of the server pool. For example, `oim-pool`
   - **Origin Server Type**: The type of requests the pool handles. For example, `HTTP`.
   - **Address Family**: The way OTD communicates with the origin servers. This is normally set to `inet`.

   Click **Next**.
6. Enter the following information in the Origin Server Information screen:
   - **Origin Server Host**: `OIMHOST1VHN1.example.com`
   - **Port**: `14000` (*`OIM_PORT`*)

   Click **Add Server**.
7. Enter the information for any other servers. For example:
   - **Origin Server Host**: `OIMHOST2VHN1.example.com`
   - **Port**: `14000` (*`OIM_PORT`*)

   Click **Next**.

   Review the information on the Review screen. If the information is correct, click **Create Server Pool**.
8. For each HTTP pool that was created and has more than one origin server, perform the additional configuration steps:
   a. Click on the newly create server pool name, for example `oim-pool`.

      The pool properties appear.
   b. Expand the **Advanced Settings**.
   c. Enable the check box **Dynamic Discovery**

      This ensures that any new cluster members added at a later date are automatically added to the OTD server pool without you having to add them manually, although it is still good practice.

      Note: You cannot use Dynamic Discovery for the OUD origin server pool (oud-pool)

      ---

   d. Click **Save**.
9. Click **Close** on the Results screen.
   - The details of the origin-server pool that you just created are displayed on the Origin-Server Pools page.

- In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking **Deploy Changes**, or you can do so later after making further changes as described in Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses."

10. Repeat these steps for the origin-server pool listed in Table 14–3.

14.2.5.2 Creating Virtual Servers

Create virtual servers using the information in Table 14–7, " Routes and Conditions".

Table 14–6 Virtual Server Information

Name	Host	Pool
login.example.com	login.example.com	origin-server-pool-1
prov.example.com	prov.example.com	soa-pool
iadadmin.example.com	iadadmin.example.com	iadadmin-pool
igdadmin.example.com	igdadmin.example.com	igdadmin-pool
igdinternal.example.com	igdinternal.example.com	oim-pool
iadinternal.example.com	iadinternal.example.com	msm-pool

Note: The `login.example.com` virtual server is created automatically when you created the configuration.

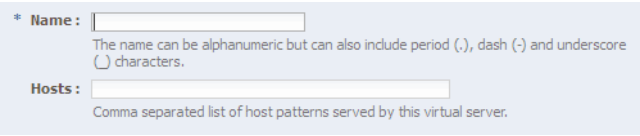
To create a virtual server using the administration console:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button that is situated at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to create a virtual server, for example `login.example.com`.
4. In the Common Tasks pane, click **New Virtual Server**.

   The New Virtual Server wizard starts.

Figure 14–3 New Virtual Server Wizard



5. On the Virtual Server Information Page enter the following information:
   - **Name**: The name describing the virtual server. For example, `login.example.com`

- **Host**: The name in the DNS/Hosts which is used to access this virtual server. For example, `login.example.com`

Click **Next**.

6. On the HTTP Listener Information screen, select the existing Listener.

   Click **Next**.

7. On the server Pool Information Screen, enter the following information:

   - **Select**: Select a pool of origin servers.
   - **Name**: Select the name of one of the server pools you created in 14.2.5.1 , "Creating OTD Origin Server Pools".

   Click **Next**.

8. Review the supplied information in the Review screen and click **Create Virtual Server**.

9. Repeat steps 4-6 for each virtual server in Table 14–6.

14.2.5.3 Creating a TCP Proxy and Listener for idstore.example.com

Create a TCP Proxy using the administration console.

To create a TCP Proxy:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":

2. Click the **Configurations** button that is situated at the upper left corner of the page.

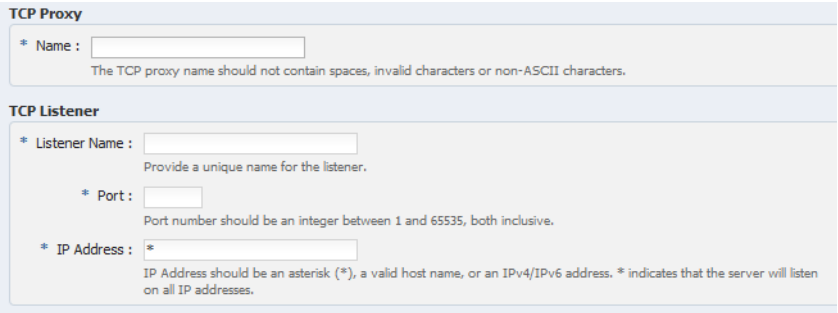
   A list of the available configurations is displayed.

3. Select the configuration for which you want to create a TCP Proxy, for example `login.example.com`.

4. In the Common Tasks pane, click **New TCP Proxy**.

   The New TCP Proxy wizard starts.

Figure 14–4 New TCP Proxy Wizard



5. In the Step 1: TCP Proxy Information screen, enter the following information and click **Next**:

   - **Name**: `idstore.example.com`
   - **Listener Name**: `listener-oud`
   - **Port**: `1389` (*`LDAP_LBR_PORT`*)

Note: If your LDAP server is running on the same host as your OTD instance, then the LDAP port (*LDAP_PORT*) and your OTD LDAP port (*LDAP_LBR_PORT*) must be different.

- In the **IP Address** field, enter *.

6. In the Step 2: Server Pool Information screen, click **Select a pool of origin servers**.
7. In the drop-down list, select **ldap-pool** and click **Next**.

   The Review screen appears.
8. Review the details and click **Create TCP Proxy**.
9. Click **Close** on the Results screen.
   - The details of the TCP Proxies that you just created are displayed on the TCP proxies page.
   - In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking **Deploy Changes**, or you can do so later after making further changes, as described in Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses."

14.2.6 Creating Routes

Note: This section is only relevant when Oracle Traffic Director is used as a web server.

Routes are similar to an Oracle HTTP location directives. Any requests received for a specific URI inside a virtual server are directed to the appropriate server pool. Adding routes allows a virtual server to direct requests to different server pools depending on what is contained within the URI.

Create the routes listed in Table 14–7using the administration console. If External Oracle HTTP Servers are being used, then routes only required for IGDINTERNAL.example.com. All other routing will take place on the Oracle HTTP Server.

Table 14–7 Routes and Conditions

Virtual Host	Route	Origin-Server Pool	Conditions	Cookie Name
iadadmin.example.com	default	iadadmin-pool	N/A	
	amaadmin-route	ama-pool	$uri= ~'/access'	
igdadmin.example.com	default	igdadmin-pool	NA	
	bi-route	bi-pool	$usr= ~'/xmlpserver'	oimjsessionid
	oim-admin-route	oim-pool	$uri =~ '/oim' or	
			$uri =~ '/identity' or	

Table 14–7 (Cont.) Routes and Conditions

Virtual Host	Route	Origin-Server Pool	Conditions	Cookie Name
			$uri =~ '/sysadmin' or $uri =~ '/xlWebApp' or $uri =~ '/Nexaweb'	
login.example.com	default	origin-server-pool-1	N/A	OAM_JSESSIONID
prov.example.com	default	soa_pool	N/A	oimjsessionid
	oim-prov-route	oim-pool	$uri =~ '/identity' or $uri =~ '/xlWebApp' or $uri =~ '/HTTPClnt' or $uri =~ '/reqsvc'	oimjsessionid
igdinternal.example.com	default	oim-pool	N/A	oimjsessionid
	soa-igdinternal-route	soa-pool	$uri =~ '/soa-infra' or $uri =~ '/sodcheck' or $uri =~ '/integration' or $uri =~ '/ucs'	oimjsessionid
iadinternal.example.com	default	iammsm-pool	N/A	

To create virtual server routes:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button that is situated at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to configure routes, for example `login.example.com`.
4. In the navigation pane, expand **Virtual Servers**, expand the **login.example.com** virtual server, and select **Routes**.

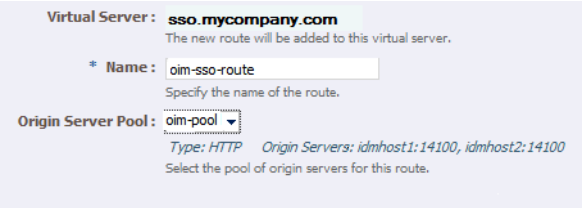
   The Routes page is displayed. It lists the routes that are currently defined for the virtual server.

   Creating a Route

   a. Click **New Route**.

      The New Route dialog box is displayed.

Figure 14–5 New Route Dialog Box



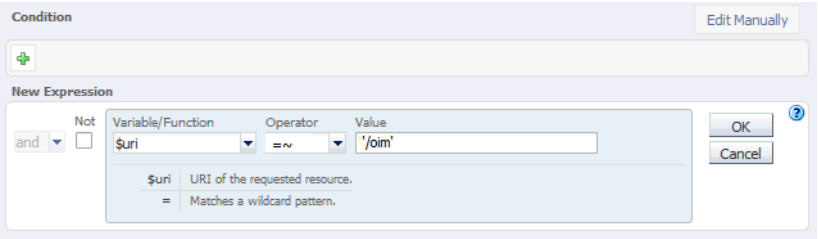
b. In the Step 1: Route Properties screen, in the **Name** field, enter `oim-sso-route`

c. In the Origin Server Pool drop-down select `oim-pool`, and click **Next**.

d. In the Step 2: Condition Information screen, select the **$uri** variable from the **Variable/Function** drop-down list. Select the Operator ('= ~ ' in your example). And enter the value in the **Value** field.

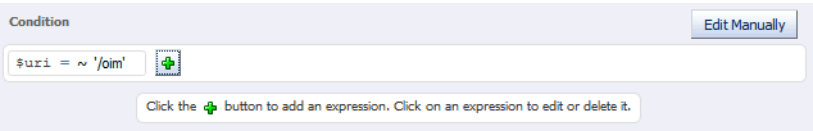
Note: Joiner, such as `and` or `or`, cannot be used for the first expression in the sequence.

Figure 14–6 New Route Condition Expressions



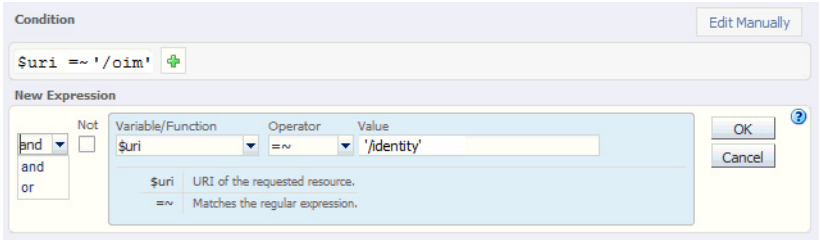
e. Click **OK** and click the **Plus** button to add the next expression.

Figure 14–7 New Route Condition Information



f. Select the **Variable/Function**, **Operator**, and **Value** and click **OK**.

Figure 14–8 New Route Condition Information



Note the joiner **'or'** can now be selected.

g. Perform steps **d** to **g** until you have added all the required values

You can also click the **Edit Manually** button to edit the expressions in a text field. Note that going into the manual mode, it is not possible to go back to the default edit mode. You must continue in the manual edit mode and save the condition.

5. Click **Next**, and then **Create Route**.

   The route that you just created is displayed on the Routes page.

   In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking **Deploy Changes**, or you can do so later after making further changes as described in Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses."

6. Update the cookie name of the newly created route and the default route:

   a. Click on the newly created route.

   b. Expand the **Advanced Settings**

   c. Set **Sticky Cookie** to the cookie name from table Table 14–7.

   d. Set the **Sticky URI Parameter** to the cookie name from Table 14–7.

   e. Repeat these steps for the values listed in Table 14–7.

   Click **Save**.

14.2.7 Enabling SSL Passthrough

In the enterprise deployment, Topology SSL is terminated at the hardware load balancer and passed through to Oracle Traffic Director using the HTTP protocol. If an external HTTP server is being used, this section is not applicable.

Oracle Traffic Director requires extra configuration steps to ensure that any application redirects occur correctly.

To ensure application redirects occur correctly:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations is displayed.

3. Select the configuration for which you want to configure routes, for example `login.example.com`.
4. In the Navigation Pane, expand **Virtual Servers** and select the virtual server **login.example.com**.
5. Click **Routes**.

   The defined routes appear.

6. Click a route, for example, **default-route**.

   The Route Properties screen appears.

7. Expand **Advanced Settings**.
8. In the **Route Properties** section, remove any content in the box labeled **Rewrite Headers**.
9. In the **Parameters Forwarded to Origin Servers** section, deselect the following:

- SSL
- Cipher
- Key Size
- Secret Key Size
- SSL/TLS Session ID
- Certificate
- User DN
- Issuer DN

Click **Save**.

10. Repeat for each route associated with the virtual server `login.example.com`.
11. Repeat for each route associated with the virtual server `prov.example.com`

14.2.8 Workaround for Issues caused by TMPWATCH cleanup

When OTD runs, it creates files in `/tmp`. The UNIX process `TMPWATCH`, which cleans up the temporary directory, can delete these files. This effects OTD's operation.

To avoid this issue, Oracle Traffic Director must be told to place its files in a location other than `/tmp`.

To do direct OTD to do this:

1. Create a directory named `tmp` in *`LOCAL_CONFIG_DIR`*, with the user same as the one that is used for running OTD Server.

   For example:

   ```
   mkdir LOCAL_CONFIG_DIR/tmp
   ```

   Create this directory on each OTD host.

2. Log in to the OTD Administration Console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs."
3. Click **Advanced Settings** from the **Configuration** menu.
4. In the **General Configuration** settings, update the value of **Temporary Directory** to *`LOCAL_CONFIG_DIR`*`/tmp`.
5. Click **Save**.

14.2.9 Deploying the Configuration and Testing the Virtual Server Addresses

Deploy the configuration to create an instance of it on an administration node. When you deploy a configuration, the running instances are reconfigured to reflect the configuration changes.

Deploying a Configuration Using the Administration Console

To deploy a configuration by using the administration console, do the following:

1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations is displayed.

3. Select **login.example.com**.
4. Click **Deploy**.

   A message is displayed confirming that the updated configuration was successfully deployed.
5. Click **Close**.

14.2.10 Creating a Failover Group for Virtual Hosts

When a request is sent to one of the virtual hosts `idstore.example.com` and `IGDINTERNAL.example.com` it is directed to the IP address associated with the virtual host name. This IP address is enabled on one of the OTD instances. In the case of failure, IP address is moved to an OTD instance that is still available.

Each OTD instance maintains a heart beat with each other OTD instance. If that heartbeat fails then OTD moves active IP addresses on the downed instance to one of the named failover instances. You do this by creating an active-passive failover group for the IP address. This failover group lists a primary and a number of secondary instances.

The enterprise deployment on Exalogic uses the following four failover groups:

- A failover group for distributing internal LDAP requests among the OUD servers.
- A failover group for internal inter-app requests.
- Two failover groups to allow the external load balancer requests among Oracle Traffic Director servers. This failover group is optional, as the load balancer could point to the OTD instances directly. The benefit of using an Oracle Traffic Director failover group is that failures are detected and resolved faster using the failover group resulting in a reduced recovery time from failed servers.

The steps below show you how to create failover groups with the information in Table 14–8.

Table 14–8 Failover Group Details

Virtual Host	Router ID	Network Prefix	Primary Node	Primary Network Interface	Secondary Node	Secondary Network Interface
idstore.example.com	50	19	Admin Node	bond0	WEBHOST2	bond0
iadinternal.example.com	52	19	WEBHOST2	bond0	Admin Node	bond0
igdinternal.example.com	53	19	Admin Node	bond0	WEBHOST2	bond0
webhost1vhn1.example.com	54	19	Admin Node	bond1	WEBHOST2	bond1
webhost2vhn1.example.com	55	19	WEBHOST2	bond1	Admin Node	bond1

Note: The failover groups for the external virtual IP addresses are optional since the load balancer fails over requests between the two Oracle Traffic Director instances. However, they will provide faster failure detection and failover than the typical load balancer monitors.

Note: The router ID is a unique number you assign to the routing. The number must be between 1 and 244.

The Network Prefix is the subnet mask in the CIDR format.

The primary node is the node where the Failover group is initially active.

The Primary Network Interface is the interface on the host where the failover group is bound.

The Secondary Node is the Node on which the failover group can be started if the Primary node is unavailable.

The Secondary Network interface is the Network Interface used on the Secondary node.

To create a failover group by using the administration console, do the following:

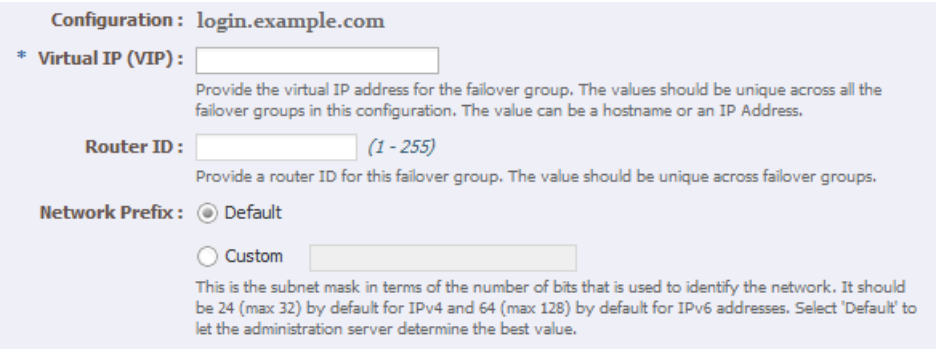
1. Log in to the OTD administration console using the URL specified in Section 31.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations appears.
3. Select the configuration for which you want to create a failover group, for example `login.example.com`.
4. In the navigation pane, click **Failover Groups**.

   The Failover Groups page is displayed.
5. Click **New Failover Group**.

   The New Failover Group wizard is displayed.

Figure 14–9 New Failover Group Wizard



6. In the **Virtual IP (VIP)** field, enter the virtual IP address associated with `idstore.example.com`. For example, 192.168.50.2. Click **Next**.

   To create the failover group for the `igdinternal.example.com` use the VIP associated with the `igdinternal.example.com` as shown in the workbook. For example, 192.168.50.1.
7. In the Step 2: Failover Nodes Information screen, select the Primary and Backup nodes, (OTDADMIN, WEBHOST2), and click **Next**.

The details of the failover group that you just created are displayed on the Failover Groups page.

Note: Generally it is sufficient to leave **Network Interface (NIC)** at the default value of `Auto Detect`. If you leave the default, Oracle Traffic Director (OTD) determines which network interface card to use based on the IP address of the failover group. If, however, this is not easily derivable, for example, if you have not used a standard CIDR associated with the IP address, you may have to manually tell OTD the network interface to which the failover group should be attached.

For example, if your internal IP address is 192.168.1.1, and it is associated with `bond0`, and uses a valid net mask (CIDR), and your IP address of the failover group is 192.168.50.1, OTD knows to use network interface `bond0`. If, however, OTD cannot determine the appropriate interface, you are required to specify it in this field.

Oracle Traffic Director validates the information before creating the failover group.

If you receive a validation error similar to the following, the IP Address you are trying to assign is incompatible with the current configuration of the network card. If you see this error you will have to choose a different IP Address/netmask:

```
OTD-67322 The specified virtual IP 'x.x.x.x' cannot be bound to any
of the network interfaces on the node 'hostname'.
The IP addresses bound to the node are [......] check if the
specified virtual IP is in the proper subnet.
This error could also be caused if either the network interfaces on
the node are not configured correctly or if the network prefix
length is incorrect.
```

---

8. Click **Close** on the Results screen.

   The details of the failover group that you just created are displayed on the Failover Groups page.

Note: A message may be displayed indicating that the failover group could not be started in the involved nodes due to insufficient privileges. To resolve this, log in to each node as root and run the following command:

```
OTD_ORACLE_HOME/bin/tadm start-failover --instance-home=WEB_
INSTANCE_HOME/ --config=login.example.com
```

14.3 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 31.1, "Starting and Stopping Enterprise Deployment 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 31.1, "Starting and Stopping Enterprise Deployment Components."

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

Back up the Oracle Traffic director configuration. For more information, see Section 31.5, "Performing Backups and Recoveries."

15

Creating Domains for an Enterprise Deployment

This section describes how to create the various domains to support the split domain topology.

> **Note:** Tasks in each section must be performed for every domain being created, unless otherwise stated.

This section contains the following topics:

15.1 Choosing Which Domains to Create

Which domains you need to create depends on the topologies that you are implementing. Table 15–1 shows which domains are required for Oracle Access Manager and Oracle Identity Manager.

Table 15–1 Domains to Create for Each Product

Domain	Virtual Host
IAMAccessDomain	IADADMINVHN.example.com
IAMGovernanceDomain	IGDADMINVHN.example.com

15.2 Domains and URLs

Table 15–2 lists the component URL's related to the domains, and the user names used to access them. In addition, Table 15–3 lists the post-Web tier configuration user names you would use to access the consoles after they have been integrated into single sign-on.

The URL's are divided into two sections:

- Pre-Web Integration
- Post-Web Integration

The rest of this document will relate to these URL's for example if you see log into the WebLogic console you will need to use the URL for the WebLogic console listed below for the domain you are working on.

Table 15–2 URLs Available Prior to Web Tier Integration

Domain	Component	URL	User
IAMAccessDomain	WebLogic Console	`http://IADADMINVHN.example.com:7001/console`	`weblogic`
	OAM Console	`http://IADADMINVHN.example.com:7001/oamconsole`	`weblogic`
	Fusion Middleware Control	`http://IADADMINVHN.example.com:7101/em`	`weblogic`
IAMGovernanceDomain	WebLogic Console	`http://IGDADMINVHN.example.com:7101/console`	`weblogic`
	Fusion Middleware Control	`http://IGDADMINVHN.example.com:7101/em`	`weblogic`

Table 15–3 URLs Available After Web Tier Integration

Domain	Component	URL	User	SSO User
IAMAccessDomain	WebLogic Console	`http://iadadmin.example.com/console`	weblogic	weblogic_idm
	Fusion Middleware Control	`http://iadadmin.example.com/em`	weblogic	weblogic_idm
	OAM Console	`http://iadadmin.example.com/oamconsole`	weblogic	oamadmin
	Policy Manager	`http://iamadmin.example.com/access`	weblogic	oamadmin
IAMGovernanceDomain	WebLogic Console	`http://igdadmin.example.com/console`	weblogic	weblogic_idm
	Fusion Middleware Control	`http://igdadmin.example.com/em`	weblogic	weblogic_idm

15.3 Running the Configuration Wizard to Create a Domain

Run the WebLogic Configuration Wizard once for each domain listed in Table 15–1.

Note: For ease of use, the example host names in this section refer to the hosts in the distributed topology. Refer to the Enterprise Deployment Workbook for that actual host names to use. For more information, see Chapter 4, "Using the Enterprise Deployment Workbook".

Table 15–4 Domains to be Created

Domain Name	Consolidated Host	Distributed Host	Listen Address	Listen Port
IAMAccessDomain	IAMHOST1	OAMHOST1	IADADMINVHN.example.com	7001
IAMGovernanceDomain	IAMHOST2	OIMHOST1	IGDADMINVHN.example.com	7101

To create a domain:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, all instances should be running, so that the validation check later in the procedure is more reliable.
2. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

   ```
   cd MW_HOME/oracle_common/common/bin
   ```

   In this command, *MW_HOME* is:

   IAD_MW_HOME for IAMAccessDomain

   IGD_MW_HOME for IAMGovernanceDomain
3. Start the Configuration Wizard using the following command:

   ```
   ./config.sh
   ```
4. On the Welcome screen, select **Create a New WebLogic Domain**, and click **Next**.
5. On the Select Domain Source screen, select the following products:

Table 15–5 Domain Component Information

Domain Name	Products
IAMAccessDomain	Oracle Access Management and Mobile Security Suite (select this and all dependent components will be selected automatically) Oracle Enterprise Manager [oracle_common] Oracle JRF [oracle_common] Oracle WSM Policy Manager [oracle_common] Oracle Platform Security Service Oracle OPSS Metadata for JRF [oracle_common]

Table 15–5 (Cont.) Domain Component Information

Domain Name	Products
IAMGovernanceDomain	Oracle Identity Manager [*IGD_ORACLE_HOME*] (select this and all dependent components will be automatically selected) Oracle Enterprise Manager [oracle_common] Oracle JRF [oracle_common] Oracle JRF WebServices Asynchronous services [oracle_common] Oracle BI Publisher [*oracle_bip*] Oracle BI JDBC [*oracle_bip*] Oracle OPSS Metadata for JRF [oracle_common] Oracle Platform Security Service [*IGD_ORACLE_HOME*] Oracle SOA Suite [*SOA_ORACLE_HOME*] Oracle WSM Policy Manager

Click **Next**.

6. On the Specify Domain Name and Location screen, enter the following:

   Domain name: Name of the Domain you are creating. For example: IAMAccessDomain

   Domain location: *SHARED_CONFIG_DIR*/domains

   Application Location: *SHARED_CONFIG_DIR*/domains/IAMAccessDomain/applications

   Ensure that the domain directory matches the directory and shared storage mount point

   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 the JDK in *MW_HOME*/jdk (for the domain you are creating. For example *IAD_MW_HOME*/jdk)

   Click **Next**.

Note: The next step and all steps through Step 12, "On the Test Component Schema," are only relevant if the domain being created is IAMAccessDomain or IAMGovernanceDomain.

---

9. On the Configure JDBC Component Schema screen, select all the data sources listed on the page.

   Select: **Convert to GridLink**.

   Click **Next**.

10. The Gridlink RAC Component Schema screen appears. In this screen, enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.

    Driver: Select **Oracle's driver (Thin) for GridLink Connections,Versions:10 and later.**

    Select **Enable FAN**.

    Do one of the following:

    - If **SSL** is not configured for ONS notifications to be encrypted, deselect **SSL**.
    - Select **SSL** and provide the appropriate wallet and wallet password.

    Service Listener: Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the parameter `remote_listener` in the database:

```
SQL>show parameter remote_listener;

NAME            TYPE   VALUE
------------------------------------------------------------
remote_listener string db-scan.example.com:1521
```

    Note:

    - For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener, for example: DBHOST1-vip.example.com (port 1521) and DBHOST2-vip.example.com (port 1521)
    - For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database.

    ONS Host: Enter the SCAN address for the Oracle RAC database and the ONS remote port, as reported by the database when you invoke the following command:

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

    Note: For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example: `DBHOST1.example.com` (port 6200) and `DBHOST2.example.com` (port 6200).

Table 15–6 RAC Component Schema Information

Domain	Schema	Service Name	User Name	Password
IAMAccess Domain	OAM Infrastructure	iadedg.example.com	EDGIAD_OAM	password
	OPSS Schema	iadedg.example.com	EDGIAD_OPSS	password
	OMSM MDS Schema	iadedg.example.com	EDGIAD_MDS	password
	OMSM Schema	iadedg.example.com	EDGIAD_OMSM	password
IAMGovernanceDomain	OIM Schema		EDGIGD_OIM	password
	SOA Infrastructure	igdedg.example.com	EDGIGD_SOAINFRA	password
	User Messaging Service	igdedg.example.com	EDGIGD_ORASDPM	password
	BIP Schema	igdedg.example.com	EDGIGD_BIPLATFORM	password
	OIM MDS Schema	igdedg.example.com	EDGIGD_MDS	password
	OWSM MDS Schema	iadedg.example.com	EDGIGD_MDS	password
	SOA MDS Schema	igdedg.example.com	EDGIGD_MDS	password
	OPSS Schema	igdedg.example.com	EDGIGD_OPSS	password

Click **Next**.

11. 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.
12. On the Select Optional Configuration screen, select the following:
    - Administration Server
    - JMS Distributed Destination (IAMGovernanceDomain only)
    - Managed Servers, Clusters and Machines
    - JMS File Store (IAMGovernanceDomain only)

    Click **Next**.
13. On the Configure the Administration Server screen, enter the following values:

    For IAMAccessDomain:

    - **Name**: *AdminServer*
    - **Listen Address**: See Table 15–4
    - **Listen Port**: See Table 15–4
    - **SSL Listen Port**: n/a
    - **SSL Enabled** (deselected)

    Click **Next**.

14. On the JMS Distributed Destination screen (IAMGovernanceDomain Only), ensure that all the JMS system resources listed on the screen are uniform distributed destinations. If they are not, select **UDD** from the drop down box. Ensure that the entries are correct according to Table 15–7.

Table 15–7 JMS Distributed Destination Information

JSM System Resource	Uniform/Weighted Distributed Destination
JRFWSASYNCJMSMODULE	UDD
BIPJMSRESOURCE	UDD
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.

15. When you first enter the Configure Managed Servers screen you will see a number of managed servers already created. DO NOT remove any of these entries. Edit the existing entries and add new ones as described below, existing entries can be matched up using ports:

Table 15–8 Consolidated WebLogic Managed Server Information

Domain	Name	Listen Address (Distributed)	Listen Address (Consolidated)	Listen Port	SSL Listen Port	SSL Enabled
IAMAccessDomain	WLS_OAM1	OAMHOST1.example.com	IAMHOST1.example.com	14100	N/A	No
	WLS_OAM2	OAMHOST2.example.com	IAMHOST2.example.com	14100	N/A	No
	WLS_AMA1	OAMHOST1.example.com	IAMHOST1.example.com	14150	N/A	No
	WLS_AMA2	OAMHOST2.example.com	IAMHOST2-.example.com	14150	N/A	No
	WLS_MSM1	OAMHOST1.example.com	IAMHOST1.example.com	14180	14181	Yes
	WLS_MSM2	OAMHOST2.example.com	IAMHOST2-.example.com	14180	14181	Yes

Table 15–8 (Cont.) Consolidated WebLogic Managed Server Information

Domain	Name	Listen Address (Distributed)	Listen Address (Consolidated)	Listen Port	SSL Listen Port	SSL Enabled
IAMGovernanceDomain	WLS_OIM1	OIMHOST1VHN1.example.com	OIMHOST1VHN1.example.com	14000	N/A	No
	WLS_OIM2	OIMHOST2VHN1.example.com	OIMHOST2VHN1.example.com	14000	N/A	No
	WLS_SOA1	OIMHOST1VNH2.example.com	OIMHOST1VHN2.example.com	8001	N/A	No
	WLS_SOA2	OIMHOST2VNH2.example.com	OIMHOST2VHN2.example.com	8001	N/A	No
	WLS_BI1	OIMHOST1VNH3.example.com	OIMHOST1VHN3.example.com	9704	N/A	No
	WLS_BI2	OIMHOST2VNH3.example.com	OIMHOST2VHN3.example.com	9704	N/A	No

Click **Next**.

Note: When using Exalogic, ensure that you set the listen address to that associated with the network interface name. For example, `IAMHOST1-INT` for the internal IPoIB network.

16. On the Configure Clusters screen, create clusters as described below by clicking Add and supplying the following information.

Table 15–9 WebLogic Cluster Information

Domain Name	Name	Cluster Messaging Mode	Muiticast Address	Multicast Port	Cluster Address
IAMAccessDomain	cluster_oam	unicast	N/A	N/A	
	cluster_ama	unicast	N/A	N/A	
	cluster_msm	unicast	N/A	N/A	
IAMGovernanceDomain	cluster_oim	unicast	N/A	N/A	OIMHOST1VHN1:14000,OIMHOST2VHN1:14000
	cluster_soa	unicast	N/A	N/A	OIMHOST1VHN2:8001, OIMHOST2VHN2:8001
	cluster_bi	unicast	N/A	N/A	OIMHOST1VHN3:9704, OIMHOST2VHN3:9704

Click **Next**.

17. On the Assign Servers to Clusters screen, associate the managed servers with the cluster as shown below. Click the cluster name in the right pane. Click the managed server under **Servers** and then click the arrow to assign it to the cluster.

Table 15–10 WebLogic Cluster Details

Cluster	Domain	Managed Servers
cluster_oam	IAMAccessDomain	WLS_OAM1 WLS_OAM2
cluster_ama	IAMAccessDomain	WLS_AMA1 WLS_AMA2
cluster_msm	IAMAccessDomain	WLS_MSM1 WLS_MSM2
cluster_oim	IAMGovernanceDomain	WLS_OIM1 WLS_OIM2
cluster_soa	IAMGovernanceDomain	WLS_SOA1 WLS_SOA2
cluster_bi	IAMGovernanceDomain	WLS_BI1 WLS_BI2

Click **Next**.

18. On the Configure Machines screen, click the **Unix Machine** tab and then click **Add** to add the following machines. 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.

    You create one machine per host in your topology, and an additional Adminhost entry for the Administration Server.

Table 15–11 Distributed WebLogic Machine Information

Domain	Name	Node Manager Listen Address	Node Manager Listen Port
IAMAccessDomain	ADMINHOST	LOCALHOST	5556
	OAMHOST1.example.com	OAMHOST1.example.com	5556
	OAMHOST2.example.com	OAMHOST2.example.com	5556
IAMGovernanceDomain	ADMINHOST	LOCALHOST	5556
	OIMHOST1.example.com	OIMHOST1.example.com	5556
	OIMHOST2.example.com	OIMHOST2.example.com	5556

Table 15–12 Consolidated WebLogic Machine Information

Domain	Name	Node Manager Listen Address	Node Manager Listen Port
IAMAccessDomain	ADMINHOST	LOCALHOST	5556
	IAMHOST1.example.com	IAMHOST1.example.com	5556
	IAMHOST2.example.com	IAMHOST2.example.com	5556
IAMGovernanceDomain	ADMINHOST	LOCALHOST	5556
	IAMHOST1.example.com	IAMHOST1.example.com	5556
	IAMHOST2.example.com	IAMHOST2.example.com	5556

Note: If you see a machine called localhost, remove it.

When using Exalogic, ensure that you set the listen address to that associated with the network interface name. For example, `IAMHOST1-INT` for the internal IPoIB network.

Click **Next**.

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

Table 15–13 Machine Names

Machine Name (Distributed)	Machine Name (Consolidated)	Managed Servers
AdminHost	AdminHost	Admin Server
OAMHOST1.example.com	IAMHOST1.example.com	WLS_OAM1 WLS_AMA1 WLS_MSM1
OAMHOST2.example.com	IAMHOST2.example.com	WLS_OAM2 WLS_AMA2 WLS_MSM2
AdminHost	AdminHost	Admin Server
OIMHOST1.example.com	IAMHOST1.example.com	WLS_SOA1 WLS_OIM1 WLS_BI1
OIMHOST2.example.com	IAMHOST2.example.com	WLS_SOA2 WLS_OIM2 WLS_BI2

Click **Next**.

20. On the Configure JMS File Stores screen (IAMGovernanceDomain only), update the directory locations for the JMS file stores. Provide the information shown in the following table.

Table 15–14 JMS File Stores Information

Name	Directory
BipJmsStore	*RT_HOME*/domains/IAMGovernanceDomain/jms/BipJmsStore
UMSJMSFileStore_auto_1	*RT_HOME*/domains/IAMGovernanceDomain/jms/UMSJMSFileStore_auto_1
UMSJMSFileStore_auto_2	*RT_HOME*/domains/IAMGovernanceDomain/jms/UMSJMSFileStore_auto_2
BPMJMSServer_auto_1	*RT_HOME*/domains/IAMGovernanceDomain/jms/BPMJMSServer_auto_1
BPMJMSServer_auto_2	*RT_HOME*/domains/IAMGovernanceDomain/jms/BPMJMSServer_auto_2
SOAJMSFileStore_auto_1	*RT_HOME*/domains/IAMGovernanceDomain/jms/SOAJMSFileStore_auto_1
SOAJMSFileStore_auto_2	*RT_HOME*/domains/IAMGovernanceDomain/jms/SOAJMSFileStore_auto_2
OIMJMSFileStore_auto_1	*RT_HOME*/domains/IAMGovernanceDomain/jms/OIMJMSFileStore_auto_1
OIMJMSFileStore_auto_2	*RT_HOME*/domains/IAMGovernanceDomain/jms/OIMJMSFileStore_auto_2
JRFWSASYNCFILESTORE_AUTO_1	*RT_HOME*/domains/IAMGovernanceDomain/jms/JRFWSAsyncFileStore_auto_1
JRFWSASYNCFILESTORE_AUTO_2	*RT_HOME*/domains/IAMGovernanceDomain/jms/JRFWSAsyncFileStore_auto_2

Note: The directory locations above must be on shared storage and accessible from OIMHOST1 and OIMHOST2.

Click **Next**.

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

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

15.4 Post-Configuration and Verification Tasks

After configuring the domain with the configuration Wizard, follow these instructions for post-configuration and verification, for each domain created.

This section contains the following topics:

15.4.1 Associating the Domain with the OPSS policy Store

You must associate the domain with the OPSS policy store in the database. This is must be done before a domain is started.

To associate the domain IAMAccessDomain with the OPSS security store use the following command:

```
ORACLE_COMMON_HOME/common/bin/wlst.sh IAD_ORACLE_
HOME/common/tools/configureSecurityStore.py -d IAD_ASERVER_HOME -c IAM -m create
-p opss_schema_password
```

To associate the domain IAMGovernanceDomain with the OPSS security store use the following command:

```
ORACLE_COMMON_HOME/common/bin/wlst.sh IGD_ORACLE_
HOME/common/tools/configureSecurityStore.py -d IGD_ASERVER_HOME -c IAM -m create
-p opss_schema_password
```

Validate that the above commands have been successful by issuing the command:

```
ORACLE_COMMON_HOME/common/bin/wlst.sh IAD_ORACLE_
HOME/common/tools/configureSecurityStore.py -d IAD_ASERVER_HOME -m validate

OR

ORACLE_COMMON_HOME/common/bin/wlst.sh IGD_ORACLE_
HOME/common/tools/configureSecurityStore.py -d IGD_ASERVER_HOME -m validate
```

15.4.2 Forcing the Managed Servers to use IPv4 Networking

Manually add the system property -Djava.net.preferIPv4Stack=true to the startWebLogic.sh script, which is located in the bin directory of *ASERVER_HOME*/bin of the domain you are modifying, using a text editor as follows:

1. Locate the following line in the startWebLogic.sh script:

   ```
   {DOMAIN_HOME}/bin/setDomainEnv.sh $*
   ```

2. Add the following property immediately after the above entry:

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.net.preferIPv4Stack=true"
   ```

3. Save and close the file.
4. Complete the procedure for each domain.

15.4.3 Setting IAMAccessDomain Memory Parameters

In the IAMAccessDomain the initial startup parameters which define memory usage are insufficient. These parameters need to be increased.

To edit the setDomainEnv.sh file to change memory allocation setting:

1. Open the setDomainEnv.sh file located in the following directory using a text editor: *IAD_ASERVER_HOME*/bin.
2. Change the following memory allocation by updating the Java maximum memory allocation pool (Xmx) to 3072m and initial memory allocation pool (Xms) to 1024m. For example, change the following line to be:

   ```
   WLS_MEM_ARGS_64BIT="-Xms1024m -Xmx3072m"
   ```

   Update the values of the following parameters as specified:

   ```
   XMS_JROCKIT_64BIT="1024"
   XMX_JROCKIT_64BIT="3072"
   XMS_SUN_64BIT="1024"
   XMX_SUN_64BIT="3072"
   ```

   Save the file when finished.

15.4.4 Creating boot.properties for the WebLogic Administration Servers

Create a boot.properties file for each Administration Server. This file will be placed into the *ASERVER_HOME*/servers/AdminServer directory of each domain (IAD/IGD). If the file already exists, edit it. 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 ASERVER_HOME/servers/AdminServer/security
   ```

   Where *ASERVER_HOME* is the *SHARED_CONFIG_DIR* domain directory that corresponds with that Administration Server: IAMAccessDomain or IAMGovernanceDomain.

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
```

3. Save the file and close the editor.

> **Note:** The username and password entries in the file are not encrypted until you start the Administration Server. 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.

15.4.5 Perform Initial Node Manager Configuration

One Node Manager runs per host, regardless of the number of domains being supported by that host. Node Manager uses content from the *MW_HOME*/wlserver_10.3 directory. If you are running a consolidated topology where Access and Governance components run on the same host, you must start node manager from one of the MW_HOMEs.

The steps in this section apply to the Middleware home of your choice. These steps are for initial boot strapping. Further node manager configuration steps are described in Chapter 16, "Setting Up Node Manager for an Enterprise Deployment".

The following sections refer to just *MW_HOME* or *ASERVER_HOME*, to make it generic. If you are using Node Manager from the *IAD_MW_HOME*, the values would be *IAD_MW_HOME* or *IAD_ASERVER_HOME*. If are using the Node Manager from the *IGD_MW_HOME*, then IGD prefix should be used.

> **Note:** Perform the tasks in this section only if you have not configured the Node Manager on the host yet.
>
> For example, if you are running a consolidated topology, and if you have already created a domain and configured the Node Manager for that host and any subsequent hosts in the following chapter, you do have to perform the tasks in this section.

Perform the following tasks to set the initial Node Manager configuration:

1. Section 15.4.5.1, "Starting Node Manager"
2. Section 15.4.5.2, "Updating the Node Manager Credentials"
3. Section 15.4.5.3, "Disabling Host Name Verification"
4. Section 15.4.5.4, "Restart the Administration Server via Node Manager"
5. Section 15.4.5.5, "Validating the WebLogic Administration Server"

15.4.5.1 Starting Node Manager

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. Setting the memory parameters is required only for the first start operation. You must start the Node Manager only once per Administration Server host.

Note: This procedure assumes that you have applied WebLogic Server patch `13964737`. For more information, see:

- "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes for Identity Management*
- Section 16.1, "Recreating WebLogic Demo Certificates"

Before you start the Node Manager, edit the *MW_HOME*`/wlserver_10.3/server/bin/startNodeManager.sh` as follows:

1. Open the `startNodeManager.sh` file in an editor and locate the line starting with:

   ```
   . "${WL_HOME}/common/bin/commEnv.sh"
   ```

2. Add the following line below the line that you located in the previous step:

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.ssl.JSSEEnabled=true
   -Dweblogic.security.SSL.enableJSSE=true"
   ```

   It is recommended that you perform this step from both *IAD_MW_HOME* and *IGD_MW_HOME*.

3. Save the file.

Perform these steps to start Node Manager on the administration host:

1. Start the Node Manager to generate an initial property file. To do this, run the following commands:

   ```
   MW_HOME/wlserver_10.3/server/bin/startNodeManager.sh
   ```

2. Stop the Node Manager by killing the process.
3. Update the generated Node Manager Property file by running the following commands:

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

   This adds an extra parameter called `startScriptEnabled` to the property file. This ensures that, when the Administration Server is started, it uses the `startWebLogic.sh` script.

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

   If you are creating a distributed topology, *MW_HOME* refers to the MW_HOME of the component that will be run on that machine. For example, OAMHOST will use IAD_MW_HOME.

   If you are creating a consolidated topology, set MW_HOME to be the home that you are running Node Manager out of. Only one Node Manager can run on a given server.

4. Restart the Node Manager using the instructions mentioned in the first step.

15.4.5.2 Updating the Node Manager Credentials

You must update each domain with Node Manager administration credentials. This is done via the WebLogic Administration Console which must first be started. 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.

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

   Note: As part of application of WebLogic patch 13964737: SU Patch [YVDZ], you should have added Java arguments to various system shell scripts to enable JSSE. Refer to Section 16.1, "Recreating WebLogic Demo Certificates" for updating the scripts *ASERVER_HOME*`/bin/startWeblogic.sh` and *MW_HOME*`/wlserver_10.3/common/bin/wlst.sh`.

   ```
   cd ASERVER_HOME/bin

   ./startWebLogic.sh
   ```

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

   a. In a browser, access the WebLogic Administration console.

      ```
      http://IADADMINVHN.example.com:7001/console
      or
      http://IGDADMINVHN.example.com:7101/console
      ```

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

   c. Click **Lock & Edit.**

   d. Click *domain_name*.

   e. Select **Security** tab, and then **General** tab.

   f. Expand **Advanced Options.**

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

   h. Click **Save**.

   i. Click **Activate Changes**

15.4.5.3 Disabling Host Name Verification

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. (See Chapter 16, "Setting Up Node Manager for an Enterprise Deployment") 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 enterprise deployment topology configuration is complete.

To disable host name verification, complete the following steps for each domain:

1. Log in to the Oracle WebLogic Server Administration console.
2. Log in as the user `weblogic`, using the password you specified during the installation.
3. Click **Lock & 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**.

15.4.5.4 Restart the Administration Server via Node Manager

1. Stop the WebLogic Administration Server by issuing the command stopWebLogic.sh located under the following directory:

   ASERVER_HOME/bin

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

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

   Once in the WLST shell, execute the following commands:

   ```
   nmConnect('Admin_User','Admin_Pasword', 'ADMINHOST1','5556', 'domain_
   name','ASERVER_HOME')
   nmStart('AdminServer')
   ```

   Where domain_name is the name of the domain, `Admin_user` and `Admin_Password` are the Node Manager username and password you entered in Step 2. For example:

   ```
   nmConnect('weblogic','password', 'OAMHOST1','5556',
     'IAMAccessDomain','ASERVER_HOME')
   nmStart('AdminServer')
   ```

15.4.5.5 Validating the WebLogic Administration Server

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

1. In a browser, log in to the Oracle WebLogic Server Administration Console for example:

   ```
   http://IADADMINVHN.example.com:7001/console
   or
   http://IGDADMINVHN.example.com:7101/console
   ```

2. Log in as the WebLogic administrator, for example: `weblogic`.
3. Check that you can access Oracle Enterprise Manager Fusion Middleware Control for example:

   ```
   http://IADADMINVHN.example.com:7001/em
   or
   http://IGDADMINVHN.example.com:7101/em
   ```

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

15.4.6 Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server

Use the pack and unpack commands to separate the domain directory used by the Administration Server from the domain directory used by the managed servers. Before running the unpack script, be sure the following directories exist:

IAD_MSERVER_HOME
IGD_MSERVER_HOME

To create a separate domain directory on IAMAccessDomain:

1. Run the following command from the location *IAD_MW_HOME*/oracle_common/common/bin to create a template pack:

   ```
   ./pack.sh -managed=true -domain=IAD_ASERVER_HOME -template=domaintemplate.jar
   -template_name=domain_template
   ```

2. Run the following command from the location *IAD_MW_HOME*/oracle_common/common/bin to unpack the template in the managed server domain directory:

   ```
   ./unpack.sh -domain= IAD_MSERVER_HOME -template=domaintemplate.jar -app_
   dir=IAD_MSERVER_HOME/applications
   ```

   Note: You must have write permissions on the following directory before running the unpack command:

   LOCAL_CONFIG_DIR/domains/

3. If you already have a domain or Managed Servers running on this host, ensure that the *SHARED_CONFIG_DIR*/nodemanager/hostname/nodemanager.domains has an entry for the domain you are creating. This entry should point to the *MSERVER_HOME* directory.

   If the entry is missing, you must enrol the domain with the running Node Manager. To do this, perform the following steps:

   1. Launch the WebLogic Scripting Tool (WLST) using the following command from the location *MW_HOME*/oracle_common/common/bin:

      ```
      ./wlst.sh
      ```

   2. Connect to the domain you wish to add, by running the following command:

      ```
      connect('weblogic_user','password','t3://ADMINVHN:AdminPort')
      ```

In this command:

weblogic_user is the WebLogic Administration user. For example, weblogic or weblogic_idm.

password is the password of the WebLogic Administrator account.

ADMINVHN is the virtual host name of Administration Server. For example, IGDADMINVHN or IADADMINVHN.

adminPort is the port on which the Administration Server is running. For example, 7101.

For example:

```
connect('weblogic_idm','mypasswd','t3://igdadminvhn.example.com:7001')
```

3. Enrol the domain using the following command:

```
nmEnroll(domainDir=full_path_to_the_domain,nm_Home=full_path_to_
the_nodemanager_home)
```

For example:

```
nmEnroll(domainDir='/u02/private/oracle/config/domains/IAMGovernanceDomain/
',nmHome='/u01/oracle/config/nodemanger/hostname')
```

Note: For Managed Servers, the domain home must be specified as the local Managed Server directory.

15.4.7 Propagating Changes to Remote Servers

Before you can start managed servers on remote hosts, you must first perform an unpack on those servers.

IAMAccessDomain should be unpacked on OAMHOST2 and IAMGovernanceDomain should be unpacked on host OIMHOST2.

Using the file domaintemplate.jar created above perform an unpack on the target host by using the following commands:

```
cd IAD_MW_HOME/oracle_common/common/bin
./unpack.sh -domain= IAD_MSERVER_HOME
-template=domaintemplate.jar -app_dir=IAD_MSERVER_HOME/applications
```

15.4.8 Starting Node Manager on Remote Servers

Start the Node Manager on OIMHOST1, OIMHOST2, OAMHOST1, and OAMHOST2, if not already started.

For information about starting the Node Manager, see Section 31.1.4.1, "Starting Node Manager".

15.4.9 Configuring the Web Tier

This section of the document describes how to access the WebLogic Administration services via the Web Server. The Web Server will be either Oracle HTTP Server or Oracle Traffic Director depending on your topology.

Perform the following tasks to configure Web Tier:

1. Section 15.4.9.1, "Registering Oracle HTTP Server with Oracle WebLogic Server"
2. Section 15.4.9.2, "Setting the Front End URL for the Administration Console"
3. Section 15.4.9.3, "Enabling WebLogic Plug-in"
4. Section 15.4.9.4, "Validating Access to Domains"

15.4.9.1 Registering Oracle HTTP Server with Oracle WebLogic Server

This step is optional.

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 IAMAccessDomain. To do this, register Oracle HTTP Server with Oracle WebLogic Server by running the following command on WEBHOST1 from the location *OHS_ORACLE_INSTANCE*/bin:

```
./opmnctl registerinstance -adminHost IADADMINVHN.example.com -adminPort
7001 -adminUsername WebLogic
```

Run this command for ohs2 on WEBHOST2. This step is optional. Each Oracle HTTP Server can be registered with only one domain.

15.4.9.2 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 the 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. Go to the **Protocols** tab, and then to the **HTTP** tab.
7. Set the **Front End Host** and **Front End HTTP PORT** fields to your load balancer address as shown in

Table 15–15 Front End URL Information

DOMAIN	FRONT END HOST	FRONT END HTTP PORT
IAMAccessDomain	iadadmin.example.com	80
IAMGovernanceDomain	igdadmin.example.com	80

8. Click **Save**, and then click **Activate Changes**.

To eliminate redirections, the best practice is to disable the Administration console's Follow changes feature. To do this, log in to the administration console and click

Preference, and then click **Shared Preferences**. Deselect **Follow Configuration Changes**, and click **Save**.

15.4.9.3 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.
2. Click **Lock and Edit**.
3. Click ***domain_name***, for example: **IAMAccessDomain** in the Domain Structure Menu.
4. Go to the **Configuration** tab.
5. Go to the **Web Applications** sub tab.
6. Select **WebLogic Plugin Enabled**.
7. Click **Save**, and then click **Activate Changes**.
8. Restart the WebLogic Administration Server.

15.4.9.4 Validating Access to Domains

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.

Validate the Administration Console and the Oracle Enterprise Manager Fusion Middleware Control through Oracle HTTP Server using each of the `console` and `em` using the URLs available after Web Tier integration. For example:

```
http://iadadmin.example.com/console
http://iadadmin.example.com/em
http://igdadmin.example.com/console
http://igdadmin.example.com/em
```

15.4.10 Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment

This section provides guidelines for when to use JDBC persistent stores for transaction logs (TLOGs) and JMS. This section also provides the procedures to configure the persistent stores in a supported database.

A JDBC store can be configured when a relational database is used for storage. A JDBC store enables you to store persistent messages in a standard JDBC-capable database, which is accessed through a designated JDBC data source. The data is stored in the JDBC store's database table, which has a logical name of WLStore. It is up to the database administrator to configure the database for high availability and

performance. JDBC stores also support migratable targets for automatic or manual JMS service migration.

Using JMS in the database is optional; however, it can simplify Disaster Recovery implementations. If other servers in the same domain have already been configured with JDBC store for JMS, the same tablespace and data sources can be used. The sections below describe the steps to configure a database user and tablespace for the JDBC persistent store and a gridlink datasource in weblogic for the database schema.

Once the database schema and datasource are configured, you must create the JDBC persistent store and associate it with the gridlink datasource.

The following sections describe the process for configuring JDBC persistent store for the OIM JMS server. Same procedure can be followed to configure JDBC JMS persistence store for SOA and BI JMS servers.

- Section 15.4.10.1, "About JDBC Persistent Stores for JMS and TLOGs"
- Section 15.4.10.2, "Performance Impact of the TLOGs and JMS Persistent Stores"
- Section 15.4.10.3, "Roadmap for Configuring a JDBC Persistent Store for TLOGs"
- Section 15.4.10.4, "Roadmap for Configuring a JDBC Persistent Store for JMS"
- Section 15.4.10.5, "Creating a User and Tablespace for TLOGs"
- Section 15.4.10.6, "Creating a User and Tablespace for JMS"
- Section 15.4.10.7, "Creating GridLink Data Sources for TLOGs and JMS Stores"
- Section 15.4.10.8, "Assigning the TLOGs JDBC Store to the Managed Servers"
- Section 15.4.10.9, "Creating a JMS JDBC Store"
- Section 15.4.10.10, "Assigning the JMS JDBC Store to the JMS Servers"
- Section 15.4.10.11, "Creating the Required Tables for JMS JDBC Store"

15.4.10.1 About JDBC Persistent Stores for JMS and TLOGs

Oracle Fusion Middleware supports both database-based and file-based persistent stores for Oracle WebLogic Server transaction logs (TLOGs) and JMS. Before deciding on a persistent store strategy for your environment, consider the advantages and disadvantages of each approach.

> **Note:** Regardless of which storage method you choose, Oracle recommends that, for transaction integrity and consistency, you use the same type of store for both JMS and TLOGs.

When you store your TLOGs and JMS data in an Oracle database, you can take advantage of the replication and high availability features of the database. For example, you can use OracleData Guard to simplify cross-site synchronization. This is especially important if you are deploying Oracle Fusion Middleware in a disaster recovery configuration.

Storing TLOGs and JMS data in a database also means you do not have to identity a specific shared storage location for this data. However, the shared storage is still required for other aspects of an enterprise deployment. For example, it is necessary for Admnistration Server configuration (to support Administration Server failover), for deployment plans, and for adapter artifacts, such as the File/FTP Adapter control and processed files.

If you are storing TLOGs and JMS stores on a shared storage device, you can protect this data by using the appropriate replication and backup strategy to guarantee zero data loss, and you will potentially realize better system performance. However, the file system protection will always be inferior to the protection provided by an Oracle Database.

For more information about the potential performance impact of using a database-based TLOGs and JMS store, see Section 15.4.10.2, "Performance Impact of the TLOGs and JMS Persistent Stores".

15.4.10.2 Performance Impact of the TLOGs and JMS Persistent Stores

One of the primary considerations when selecting a storage method for Transaction Logs and JMS persistent stores is the potential impact on performance. This topic provides some guidelines and details to help you determine the performance impact of using JDBC persistent stores for TLOGs and JMS.

Performance Impact of Transaction Logs Versus JMS Stores

For transaction logs, the impact of using a JDBC store is relatively small, because the logs are very transient in nature. Typically, the effect is minimal when compared to other database operations in the system.

On the other hand, JMS database stores can have a higher impact on performance if the application is JMS intensive. For example, the impact of switching from a file-based to database-based persistent store is very low when you are using the SOA Fusion Order Demo (a sample application used to test Oracle SOA Suite environments), because the JMS database operations are masked by many other SOA database invocations that are much heavier.

Factors that Affect Performance

There are multiple factors that can affect the performance of a system when it is using JMS DB stores for custom destinations. The following are the important ones:

- Custom destinations involved and their type
- Payloads being persisted
- Concurrency on the SOA system (producers on consumers for the destinations)

Depending on the effect of each one of the above, different settings can be configured in the following areas to improve performance:

- Type of data types used for the JMS table (using raw versus lobs)
- Segment definition for the JMS table (partitions at index and table level)

Impact of JMS Topics

If your system uses Topics intensively, then, as concurrency increases, the performance degradation with an Oracle RAC database will increase more than for Queues. In tests conducted by Oracle with JMS, the average performance degradation for different payload sizes and different concurrency was less than 30% for Queues. For topics, the impact was more than 40%. Consider the importance of these destinations from the recovery perspective when deciding whether to use database stores.

Impact of Data Type and Payload Size

When choosing to use the RAW or SecureFiles LOB data type for the payloads, consider the size of the payload being persisted. For example, when payload sizes

range between 100b and 20k, then the amount of database time required by SecureFiles LOB is slightly higher than for the RAW data type.

More specifically, when the payload size reach around 4k, then SecureFiles tend to require more database time. This is because 4k is where writes move out-of-row. At around 20k payload size, SecureFiles data starts being more efficient. When payload sizes increase to more than 20k, then the database time becomes worse for payloads set to the RAW data type.

One additional advantage for SecureFiles is that the database time incurred stabilizes with payload increases starting at 500k. In other words, at that point it is not relevant (for SecureFiles) whether the data is storing 500k, 1MB, or 2MB payloads, because the write is asynchronized, and the contention is the same in all cases.

The effect of concurrency (producers and consumers) on the queue's throughput is similar for both RAW and SecureFiles until the payload sizes reeach 50K. For small payloads, the effect on varying concurrency is practically the same, with slightly better scalability for RAW. Scalability is better for SecureFiles when the payloads are above 50k.

Impact of Concurrency, Worker Threads, and Database Partioning

Concurrency and worker threads defined for the persistent store can cause contention in the RAC database at the index and global cache level. Using a reverse index when enabling multiple worker threads in one single server or using multiple Oracle WebLogic Server clusters can improve things. However, if the Oracle Database partitioning option is available, then global hash partition for indexes should be used instead. This reduces the contention on the index and the global cache buffer waits, which in turn improves the response time of the application. Partitioning works well in all cases, some of which will not see significant improvements with a reverse index.

15.4.10.3 Roadmap for Configuring a JDBC Persistent Store for TLOGs

This section lists the tasks to configure a database-based persistent store for JMS:

1. Section 15.4.10.5, "Creating a User and Tablespace for TLOGs"
2. Section 15.4.10.7, "Creating GridLink Data Sources for TLOGs and JMS Stores"
3. Section 15.4.10.8, "Assigning the TLOGs JDBC Store to the Managed Servers"

15.4.10.4 Roadmap for Configuring a JDBC Persistent Store for JMS

This section lists the tasks to configure a database-based persistent store for JMS:

1. Section 15.4.10.6, "Creating a User and Tablespace for JMS"
2. Section 15.4.10.7, "Creating GridLink Data Sources for TLOGs and JMS Stores"
3. Section 15.4.10.9, "Creating a JMS JDBC Store"
4. Section 15.4.10.10, "Assigning the JMS JDBC Store to the JMS Servers"
5. Section 15.4.10.11, "Creating the Required Tables for JMS JDBC Store"

15.4.10.5 Creating a User and Tablespace for TLOGs

Before you can create a database-based persistent store for transaction logs, you must create a user and tablespace in a supported database by completing the following steps:

1. Create a tablespace called `logs`. For example, log in to SQL*Plus as the `sysdba` user and run the following command:

```
create tablespace IAMTLOGS datafile 'DBFILE_LOCATION/IAMTLOGS.dbf' size 32m
autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `IAMTLOGS` and assign to it the `IAMTLOGS` tablespace using the following command:

```
create user IAMTLOGS identified by password;
grant create table to IAMTLOGS;
grant create session to IAMTLOGS;
alter user IAMTLOGS default tablespace IAMTLOGS;
alter user IAMTLOGS quota unlimited on IAMTLOGS;
```

15.4.10.6 Creating a User and Tablespace for JMS

To set up a user and tablespace for the JDBC Persistent store, complete the following steps:

1. Create a tablespace called `IAMJMS`. For example, log on to SQL*Plus as the `sysdba` user and run the following command:

```
create tablespace IAMJMS datafile 'DB_HOME/oradata/orcl/IAMJMS.dbf' size 32m
autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `EDGIGD_JMS` and assign to it the `IAMJMS` tablespace using the following command:

```
create user EDGIGD_JMS identified by password;
grant create table to EDGIGD_JMS;
grant create session to EDGIGD_JMS;
alter user EDGIGD_JMS default tablespace IAMJMS;
alter user EDGIGD_JMS quota unlimited on IAMJMS;
```

15.4.10.7 Creating GridLink Data Sources for TLOGs and JMS Stores

Before you can configure database-based persistent stores for JMS and TLOGs, you must create two data sources: one for the TLOGs persistent store and one for the JMS persistent store.

For an enterprise deployment, you should use GridLink data sources for your TLOGs and JMS stores. To create a GridLink data source, complete the following steps:

1. Log in to the Oracle WebLogic Server Administration Console for the IAMGovernanceDomain. The following is an example of the URL:

   `http://igdadmin.example.com:7101/console`

2. In the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the **Summary of Data Sources** page, click **New** and select **GridLink Data Source**, and enter the following information appropriate to the datasource you are creating:

Name	JNDI Name	Database Driver
IGDTLOGS_DS	jdbc/igdtlogs	Oracle's Driver (Thin) for GridLink Connections Versions: 11 and later.

Name	JNDI Name	Database Driver
IGDJMS_DS	jdbc/igdjms	Oracle's Driver (Thin) for GridLink Connections Versions: 11 and later.

Click **Next**.

5. On the **Transaction Options** page, de-select **Supports Global Transactions**, **Logging Last Resource**, and **Emulate Two Phase commit**.

   Click **Next**.

6. On the **GridLink Data Source Connection Properties Options** screen, select **Enter individual listener information**.

   Click **Next**.

7. Enter the following connection properties:

   - **Service Name**: Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example, `igdedg.example.com`
   - **Host Name and Port**: Enter the SCAN address and port for the RAC database, separated by a colon. For example:

     db-scan.example.com:1521

     Click **Add** to add the host name and port to the list box below the field.

     You can identify this address by querying the appropriate parameter in the database using the TCP Protocol:

     ```
     SQL>show parameter remote_listener;
     ```

NAME	TYPE	VALUE
remote_listener	string	db-scan.example.com

> **Note:** For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener. For example:
>
> `IDMDBHOST1-vip.example.com (port 1521)`
>
> and
>
> `IDMDBHOST2-vip.example.com (port 1521)`

   - **Port**: The port on which the database server listens for connection requests.
   - **Database User Name**: For the TLOGs store, enter **IAMTLOGS**. For the JMS persistent store, enter **EDGIGD_JMS**. For example, `EDGIGD_JMS`
   - **Password**: Enter the password you used when you created the user in the database. For example: `password`
   - **Confirm Password**: Enter the password again.

   Click **Next**.

8. On the **Test GridLink Database Connection** page, review the connection parameters and click **Test All Listeners**.

   Click **Next**.

9. On the **ONS Client Configuration** page, do the following:

   Select **FAN Enabled** to subscribe to and process Oracle FAN events.

   Enter the SCAN address for the RAC database and the ONS remote port as reported by the database. For example:

   ```
   srvctl config nodeapps -s

   ONS exists: Local port 6100, remote port 6200, EM port 2016
   ```

   Click **ADD**.

   Click **Next**.

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

   ```
   IDMDBHOST1.example.com (port 6200)
   ```

   and

   ```
   IDMDBHOST2.example.com (6200)
   ```

10. On the **Test ONS Client Configuration** page, review the connection parameters and click **Test All ONS Nodes**.

    Click **Next**.

11. On the **Select Targets** page, select **cluster_bi**, **cluster_oim**, and **cluster_soa**.

12. Click **Finish**.

13. Repeat the steps to create both the data sources.

14. Click **Activate Changes** after you create each of the data sources, or after creating both.

15.4.10.8 Assigning the TLOGs JDBC Store to the Managed Servers

After you create the tablespace and user in the database, and the datasource, you must assign the TLOGs persistence store to each of the required Managed Servers. To do this, complete the following steps:

1. Log in to the Oracle WebLogic Server Administration Console for the IAMGovernanceDomain. The following is an example of the URL:

   ```
   http://igdadmin.example.com:7101/console
   ```

2. In the **Change Center**, click **Lock and Edit**.

3. In the **Domain Structure** tree, expand **Environment**, and then **Servers**.

4. Click the name of the Managed Server you want to use the TLOGs store.

5. Select **Configuration**, and then select **General**.

6. Go to the **Services** tab.

7. Under **Transaction Log Store**, select **JDBC** from the **Type** menu.

8. From the **Data Source** menu, select the data source you created for the TLOGs persistence store.
9. In the **Prefix Name** field, specify a prefix name to form a unique JDBC TLOG store name for each configured JDBC TLOG store.
10. Click **Save**.
11. Repeat step 3 to 7 for each of the additional Managed Servers in the cluster.
12. To activate these changes, in the **Change Center** of the Administration Console, click **Activate Changes**.

15.4.10.9 Creating a JMS JDBC Store

To create a JDBC Persistent Store, complete the following steps:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Persistent Stores**.
4. On the **Summary of Persistent Stores** page, click **New**, and select **JDBC Store**, and enter the following:
   - **Name**: Name of the jdbc store. For example, `OIMJMSDBSTORE_1`
   - **Target**: wls_oim1
   - **Data Source**: `IGDJMS_DS`
   - **Prefix Name**: oimjmsdb1

   Note: It is highly recommended that you configure the Prefix option to a unique value for each configured JDBC store table.
5. Click **OK**.
6. Repeat steps 3 to 5 for the Persistent Stores listed in Table 15–16

Table 15–16 Persistent Stores

Name	Target	Datasource	Prefix
OIMJMSDBSTORE_2	wls_oim2	IGDJMS_DS	oimjmsdb2
SOAJMSDBSTORE_1	wls_soa1	IGDJMS_DS	soajmsdb1
SOAJMSDBSTORE_2	wls_soa2	IGDJMS_DS	soajmsdb2
BIJMSDBSTORE_1	wls_bi1	IGDJMS_DS	bijmsdb1
BIJMSDBSTORE_2	wls_bi2	IGDJMS_DS	bijmsdb2
BPMJMSDBSTORE_1	wls_soa1	IGDJMS_DS	bpmjmsdb1
BPMJMSDBSTORE_2	wls_soa2	IGDJMS_DS	bpmjmsdb2
JRFWSASYNCDBSTORE_1	wls_oim1	IGDJMS_DS	jrfwsasynchdb1
JRFWSASYNCDBSTORE_2	wls_oim2	IGDJMS_DS	jrfwsasynchdb2
PS6SOAJMSDBSTORE_1	wls_soa1	IGDJMS_DS	ps6soajmsdb1
PS6SOAJMSDBSTORE_2	wls_soa2	IGDJMS_DS	ps6soajmsdb2
UMSJMSDBSTORE_1	wls_soa1	IGDJMS_DS	umsjmsdb1

Table 15–16 (Cont.) Persistent Stores

Name	Target	Datasource	Prefix
UMSJMSDBSTORE_2	wls_soa2	IGDJMS_DS	umsjmsdb2

15.4.10.10 Assigning the JMS JDBC Store to the JMS Servers

To configure JMS Server to use JDBC Persistent Store, do the following:

1. In the **Domain Structure** tree, expand **Services**, **Messaging**, and then select **JMS Servers**.
2. On the **Summary of JMS Servers** page, click **OIMJMSSERVER_auto_1**, that is the JMS Server for OIM that is targeted to WLS_OIM1.
3. On the **General Configurations** page of the OIM JMS Server, update the Persistent Store to use the JDBC Persistent store OIMJMSDBSTORE_1.
4. Click **Save** and then click **Finish**.
5. Repeat steps 1 to 4 for each of the JMS data stores created in the earlier sections.
6. Click **Activate Changes**.

> **Note:** When Oracle BI Publisher is configured, only one persistent store is created. This is a know issue. To create JMS store for each of the BI Managed Servers, manually, refer to Section 20.2.2, "Configuring JMS for BI Publisher".

15.4.10.11 Creating the Required Tables for JMS JDBC Store

The final step in using a JDBC persistent store for JMS is to create the required JDBC store tables. Perform this task before restarting the Managed Servers in the domain. To do this, complete the following steps:

1. If you want to use `oracle_blob.ddl`, run the following commands to extract the `oracle_blob.ddl` file from the `com.bea.core.store.jdbc_1.3.1.0.jar` file:

   ```
   cd IGD_MW_HOME/modules

   jar -xvf com.bea.core.store.jdbc_1.3.1.0.jar weblogic/store/io/jdbc/ddl
   ```

   > **Note:** If you omit the `weblogic/store/io/jdbc/ddl` parameter, then the entire jar file is extracted.

2. Review the information in Performance Impact of the TLOGs and JMS Persistent Stores, and edit the DDL file, accordingly.

   For example, for an optimized schema definition that uses both secure files and hash partitioning, create a `jms_custom.ddl` file in the *RT_HOME* directory (or any other directory on shared storage accessible from all servers) with the following content:

   ```
   CREATE TABLE $TABLE (
     id     int  not null,
     type   int  not null,
     handle int  not null,
     record blob not null,
   PRIMARY KEY (ID) USING INDEX GLOBAL PARTITION BY HASH (ID) PARTITIONS 8)
   LOB (RECORD) STORE AS SECUREFILE (ENABLE STORAGE IN ROW);
   ```

This example can be compared to the default schema definition for JMS stores, where the RAW data type is used without any partitions for indexes.

Note that the number of partitions should be a power of two. This will ensure that each partition will be of the same size. The recommended number of partitions will vary depending on the expected table or index growth. You should have your database administrator (DBA) analyze the growth of the tables over time and adjust the tables accordingly. For more information, see the *Oracle Database VLDB and Partitioning Guide*.

3. Edit the existing JDBS Store you created earlier to create the table that will be used for the JMS data, using the Administration Console. To do this, complete the following steps:
   a. Log in to the Oracle WebLogic Server Administration Console.
   b. In the **Change Center**, click **Lock and Edit**.
   c. In the **Domain Structure** tree, expand **Services**, then expand **Persistent Stores**.
   d. Click the persistent store you created earlier.
   e. Under the **Advanced** options, enter *RT_HOME*/jms_custom.ddl in the **Create Table from DDL File** field.

      Note: You can use the oracle_blob.ddl that was extracted from com.bea.core.store.jdbc_1.3.1.0.jar or you can use a custom ddl script prepared as part of step 2.

      The oracle_blob.ddl path would be:

      IGD_MW_HOME/modules/weblogic/store/io/jdbc/ddl/oracle_blob.ddl

   f. Click **Save**.
   g. To activate these changes, in the **Change Center** of the Administration Console, click **Activate Changes**.
   h. Restart the Managed Servers.

15.4.11 Manually Failing over the WebLogic Administration Server

If a node running the Administration Server fails, you can fail over the Administration Server to another node. To do this, complete the following steps:

1. Disable the Administration Server virtual IP address on the failed server, if it is not disabled already.
2. Unmount the *ASERVER_HOME* shared file system from the failed server, if it is not dismounted already.
3. Mount the *ASERVER_HOME* shared file system on a new node.
4. Enable the Administration Server virtual IP Address on the new server.
5. Start the Administration Server.

15.4.12 Backing up the WebLogic Domain

It is recommendation that you 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 was 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 information about backing up database, see *Oracle Database Backup and Recovery User's Guide*.

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

1. Back up the web tier.
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Stop the Node Manager and all the processes running in the domain.
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.

15.4.13 Adding a Load Balancer Certificate to JDK Trust Stores

Some IAM Products require that the SSL certificate used by the load balancer be added to the trusted certificates in the JDK.

To add the certificate, do the following:

1. Create a directory to hold user created keystores and certificates. For example:

   ```
   mkdir SHARED_CONFIG_DIR/keystores
   ```

2. Obtain the certificate from the load balancer.

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

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

   For example:

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

   This command saves the certificate to a file called *login.example.com*.pem in the following directory:

   ```
   SHARED_CONFIG_DIR/keystores
   ```

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

   ```
   set JAVA_HOME to IGD_MW_HOME/jdk
   ```

```
set PATH to include JAVA_HOME/bin

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

keytool -importcert -file SHARED_CONFIG_DIR/keystores/login.example.com.pem
-trustcacerts -keystore SHARED_CONFIG_
DIR/keystores/appTrustKeyStore-oimhost1vhn1.example.com.jks

keytool -importcert -file SHARED_CONFIG_DIR/keystores/login.example.com.pem
-trustcacerts -keystore SHARED_CONFIG_
DIR/keystores/appTrustKeyStore-oimhost2vhn1.example.com.jks

keytool -importcert -file SHARED_CONFIG_DIR/keystores/login.example.com.pem
-trustcacerts -keystore SHARED_CONFIG_
DIR/keystores/appTrustKeyStore-oimhost1.example.com.jks

keytool -importcert -file SHARED_CONFIG_DIR/keystores/login.example.com.pem
-trustcacerts -keystore SHARED_CONFIG_
DIR/keystores/appTrustKeyStore-oimhost2.example.com.jks
```

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

Note: The names of the virtual hosts you assigned to your OIM server are `oimhost1vhn1` and `oimhost2vhn1`.

15.4.14 Enabling Exalogic Optimizations

This section describes the tasks specific to Exalogic optimization. This sections contains the following topic:

- Section 15.4.14.1, "Enabling WebLogic Domain Exalogic Optimization"

15.4.14.1 Enabling WebLogic Domain Exalogic Optimization

Perform these steps to enable WebLogic domain Exalogic optimizations:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Select the domain name - IAMAccessDomain or IAMGovernanceDomain, in the left navigation pane.
3. Click **Lock & Edit**.
4. On the Settings page, click the **General** tab.
5. Select **Enable Exalogic Optimizations**, and click **Save and Activate Changes**.
6. Restart the WebLogic Administration Server.

16

Setting Up Node Manager for an Enterprise Deployment

This chapter describes how to configure Node Manager in accordance with Oracle best practice recommendations.

This chapter contains the following sections:

16.1 Recreating WebLogic Demo Certificates

The security imposed by Java 7 means that the demo certificates need to be recreated with a higher level of encryption.

> **Note:** This procedure assumes you have applied WebLogic Server patch 13964737. For more information, see:
>
> - "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes for Identity Management*.
> - Section 16.1, "Recreating WebLogic Demo Certificates"

Once the patch has been installed using WebLogic smart update, the WebLogic demo certificates need to be created as follows:

1. Create a temporary working directory. For example:

   ```
   mkdir /u01/lcm/tmp
   ```

2. Set `JAVA_HOME` to *`JAVA_HOME`*.

3. Add `JAVA_HOME/bin` to your system path. For example:

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

4. Set up your WebLogic environment by executing the script `setWLSEnv.sh`. For example:

   `MW_HOME``/wlserver10.3/server/bin/setWLSEnv.sh`

5. Change directory to the temporary directory. For example:

   ```
   cd /u01/lcm/tmp
   ```

6. Regenerate the certificates using the following commands:

   ```
   java utils.CertGen -keyfilepass DemoIdentityPassPhrase -certfile
   democert -keyfile demokey -strength 2048
   ```

   ```
   java utils.ImportPrivateKey -keystore DemoIdentity.jks -storepass
   DemoIdentityKeyStorePassPhrase -keyfile demokey.der -keyfilepass
   DemoIdentityPassPhrase -certfile democert.der -alias demoidentity
   ```

7. Shutdown all of the Node Managers, Managed Servers, and the Administration Server in the domain.

8. Back up the existing certificate. For example:

   ```
   cp $MW_HOME/wlserver10.3/server/lib/DemoIdentity.jks $MW_HOME/wlserver_
   10.3/server/lib/DemoIdentity.orig
   ```

9. Move the certificate to the directory *MW_HOME*`/wlserver10.3/server/lib`. For example:

   ```
   mv DemoIdentity.jks $MW_HOME/wlserver_10.3/server/lib
   ```

10. Remove your temporary working directory.

After you create WebLogic demo certificates, you must update the shell scripts to force the use of JSEE SSL. Now that you are using the new more secure JSEE certificate methods, the following Java arguments need to be added to various system shell scripts:

1. Edit the *ASERVER_HOME*`/bin/startWeblogic.sh` file to append `-Dweblogic.ssl.JSSEEnabled=true` to the line beginning with `JAVA_OPTIONS="${SAVE_JAVA_OPTIONS}"`. For example:

   ```
   JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} -Dweblogic.ssl.JSSEEnabled=true"
   ```

   Save the file.

2. Edit the *MW_HOME*`/wlserver_10.3/common/bin/wlst.sh` file to append `-Dweblogic.security.SSL.enableJSSE=true -Dweblogic.ssl.JSSEEnabled=true` to the line beginning with `JVM_ARGS=`. For example:

   ```
   JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties ${WLST_
   PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}
   -Dweblogic.security.SSL.enableJSSE=true
   -Dweblogic.ssl.JSSEEnabled=true"
   ```

   Save the file.

16.2 Overview of the Node Manager

Node Manager enables you to start and stop the Administration Server and the Managed Servers.

The procedures described in this chapter must be performed for various components of the enterprise deployment outlined in Section 2.3, "Understanding the Primary Oracle Identity and Access Management Topology Diagrams." Variables are used in this chapter to distinguish between component-specific items:

- *WLS_SERVER*: This refers to a Managed WebLogic server for the enterprise deployment component (for example, WLS_OIM1).

- *HOST*: This refers to a host machine for the enterprise deployment component (for example, OIMHOST1).
- *VIP*: This refers to a virtual IP for the enterprise deployment component (for example, OIMHOST1VHN1).

The values to be used to these variables are provided in the component-specific chapters in this guide. Please 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 configuration and log files in a location different from the default one (which is inside the Middleware Home where Node Manager resides). See Section 16.4, "Changing the Location of the Node Manager Log".
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 16.5, "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.

16.3 Moving Node Manager to a Separate Directory

Move the Node Manager to a separate directory by doing the following:

1. Stop the Node Manager by killing the Node Manager process.
2. Move the configuration files to shared storage. While not mandatory, Oracle recommends removing the configuration files from the middleware home:
   a. Create a directory for `nodemanger` using the following command:

      ```
      mkdir -p SHARED_CONFIG_DIR/nodemanager/hostname.domain
      ```

   b. Copy all of the files in the directory *MW_HOME*`/wlserver_10.3/common/nodemanager` to the directory *SHARED_CONFIG_DIR*`/nodemanager/`*hostname.domain*.
   c. Edit the file *SHARED_CONFIG_DIR*`/nodemanager/`*hostname.domain*`/nodemanager.properties` update the directory paths in the entries `DomainsFile` and `NodeManagerHome` and `LogFile` to reference the directory *SHARED_CONFIG_DIR*`/nodemanager/`*hostname.domain*.
   d. If this host contains an Administration Server, then in addition, set the following property in `nodemanager.properties`:

      ```
      DomainRegistrationEnabled=true
      ```

   e. Create a file called `startNodeManagerWrapper.sh` with the following contents:

```
#!/bin/sh
#
# This is a wrapper script that simply invokes "startNodeManager.sh"
# script after setting the appropriate JAVA_OPTIONS environment
# variable.
#
# Note: This script is provided as a convenience since we now have
# host specific node manager home directories and we need to specify
# the -DNodeManagerHome property prior to invoking "startNodeManager.sh"
# script to start an instance of node manager process manually.
#
# $Header:
faprov/modules/provisioning/framework/src/java/oracle/apps/fnd/provisioning
/ant/taskdefs/util/startnodemanagerwrapper.template /main/3 2012/04/23
21:37:51 jjiembac Exp $
#

WLS_HOME=IAD_MW_HOME/wlserver_10.3
NM_HOME=SHARED_CONFIG_DIR/nodemanager/hostname.domain

# set an environment variable to allow node manager
# to read it's host specific configuration
JAVA_OPTIONS="-DNodeManagerHome=$NM_HOME
-Dweblogic.security.SSL.enableJSSE=true $JAVA_OPTIONS"
export JAVA_OPTIONS
exec $WLS_HOME/server/bin/startNodeManager.sh
```

f. Save the file and give it execute permissions:

```
chmod 755 startNodeManagerWrapper.sh
```

3. Repeat this for each of the hosts OAMHOST1, OAMHOST2, OIMHOST1, OIMHOST2.
4. Restart Node Manager using the command `startNodeManagerWrapper.sh`.

16.4 Changing the Location of the Node Manager Log

If not already done, update the Node manager log location. Edit the Node Manager Properties file located at *SHARED_CONFIG_DIR*/nodemanager/*hostname.domain*/nodemanager.properties. Add the new location for the log file using the following line:

```
LogFile= SHARED_CONFIG_DIR/nodemanager/hostname.domain/nodemanager.log
```

Oracle best practice is to use a location outside the *MW_HOME* directory and inside the oracle base directory under which all oracle products are installed.

Restart Node Manager for the change to take effect.

16.5 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 16.5.1, "Generating Self-Signed Certificates Using the utils.CertGen Utility"
- Section 16.5.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility"

- Section 16.5.3, "Creating a Trust Keystore Using the Keytool Utility"
- Section 16.5.4, "Adding a Load Balancer Certificate to Trust Store"
- Section 16.5.5, "Configuring Node Manager to Use the Custom Keystores"
- Section 16.5.6, "Configuring the Managed WebLogic Servers to Use Custom Keystores"
- Section 16.5.7, "Changing the Host Name Verification Setting for the Managed Servers"

16.5.1 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.example.com) and a WebLogic Managed Server listens on a virtual host name (VIP.example.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*.example.com and *VIP*.example.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. The following examples configure certificates for HOST.example.com and VIP.example.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.example.com is the address used by Node Manager and VIP.example.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). You must perform the following steps for each Managed Servers hostname and each Managed Servers virtual name (if it has one).

1. Set up your environment by running the *WL_HOME*/server/bin/setWLSEnv.sh script. In the Bourne shell, run the following commands:

   ```
   cd WL_HOME/server/bin
   . ./setWLSEnv.sh
   ```

   Verify that the *CLASSPATH* environment variable is set:

   ```
   echo $CLASSPATH
   ```

2. The directory created in Section 15.4.13, "Adding a Load Balancer Certificate to JDK Trust Stores" will be used for storing the certificates. Change directory to the keystores directory that was created using the following command:

   ```
   cd SHARED_CONFIG_DIR/keystores
   ```

3. Run the `utils.CertGen` tool from the user-defined directory to create the certificates for both *HOST*.example.com and *VIP*.example.com.

Syntax (all on a single line):

```
java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
[export | domestic] [Host_Name]
```

Examples:

```
java utils.CertGen Key_Passphrase OIMHOST1.example.com_cert
OIMHOST1.example.com_key domestic OIMHOST1.example.com
java utils.CertGen Key_Passphrase OIMHOST1VHN1.example.com_cert
OIMHOST1VHN1.example.com_key domestic OIMHOST1VHN1.example.com
```

16.5.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

Follow these steps to create an identity keystore on HOST:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, *`SHARED_CONFIG_DIR`*`/keystores`).

   Note: The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store using the `utils.ImportPrivateKey` utility.

2. On HOST, import the certificate and private key for both `HOST.example.com` and `VIP.example.com` created above, into the Identity Store. Ensure that you use a different alias for each of the certificate/key pairs imported. Syntax (all on a single line):

   ```
   java utils.ImportPrivateKey Keystore_File Keystore_Password
   Certificate_Alias_to_Use Private_Key_Passphrase
   Certificate_File
   Private_Key_File
   [Keystore_Type]]
   ```

   Examples:

   ```
   java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
   appIdentity-OIMHOST1.example.com Key_Passphrase
   SHARED_CONFIG_DIR/keystores/OIMHOST1.example.com_cert.pem SHARED_CONFIG_
   DIR/keystores/OIMHOST1.example.com_key.pem

   java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
   appIdentity-OIMHOST1VHN1.example.com Key_Passphrase
   SHARED_CONFIG_DIR/keystores/OIMHOST1VHN1.example.com_cert.pem
   SHARED_CONFIG_DIR/keystores/OIMHOST1VHN1.example.com_key.pem

   java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
   appIdentity-IGDADMINVHN.example.com Key_Passphrase
   SHARED_CONFIG_DIR/keystores/igdadminvhn.example.com_cert.pem
   SHARED_CONFIG_DIR/keystores/igdadminvhn.example.com_key.pem
   ```

16.5.3 Creating a Trust Keystore Using the Keytool Utility

Follow these steps to create the trust keystore on each host:

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the *WL_HOME*/server/lib directory to the same directory as the certificates. For example:

   ```
   cp WL_HOME/server/lib/cacerts SHARED_CONFIG_DIR/keystores/appTrustKeyStore.jks
   ```

2. The default password for the standard Java keystore is changeit. Oracle recommends always changing the default password. Use the keytool utility to do this. The syntax is:

   ```
   keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
   Original_Password
   ```

   For example:

   ```
   keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStore.jks
   -storepass changeit
   ```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *WL_HOME*/server/lib directory. This CA certificate must be imported into the appTrustKeyStore using the keytool utility. The syntax is:

   ```
   keytool -import -v -noprompt -trustcacerts -alias Alias_Name -file CA_File_
   Location -keystore Keystore_Location -storepass Keystore_Password
   ```

   For example:

   ```
   keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_
   HOME/server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass Key_
   Passphrase
   ```

16.5.4 Adding a Load Balancer Certificate to Trust Store

Add the Load balancer certificate you obtained in Section 15.4.13, "Adding a Load Balancer Certificate to JDK Trust Stores", into the Node Manager Trust Store.

Load the certificate into the Node Manager Trust Store by running the following commands to import the CA certificate file, *SHARED_CONFIG_DIR*/keystores/login.example.com.pem, into the Node Manager trust store *SHARED_CONFIG_DIR*/keystores/appTrustKeyStore.jks:

```
set JAVA_HOME to IGD_MW_HOME/jdk
set PATH to include JAVA_HOME/bin
keytool -importcert -file SHARED_CONFIG_DIR/keystores/login.example.com.pem
-trustcacerts -keystore SHARED_CONFIG_DIR/keystores/appTrustKeyStore.jks
```

16.5.5 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 *SHARED_CONFIG_DIR*/nodemanager/*hostname.domain* directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=appIdentity-OIMHOST1.example.com
```

```
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=SHARED_CONFIG_DIR/keystores/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentity-OIMHOST1.example.com
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager. For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, start Node Manager as soon as possible so that the entries get encrypted.

Note: Each Node manager must point to a different identity alias to send the correct certificate to the Administration Server. In case you are using the WL_HOME/server/bin directory to start Node Manager and have not configured separate nodemanager directories, as described in this document, then you must set different environment variables before starting Node Manager in the different nodes:

```
cd WL_HOME/server/bin
export JAVA_
OPTIONS=-DCustomIdentityAlias=appIdentity-OIMHOST1.example.com

cd WL_HOME/server/bin
export JAVA_
OPTIONS=-DCustomIdentityAlias=appIdentity-OIMHOST2.example.com
```

Make sure to specify the custom identity alias specifically assigned to each host, for example `appIdentity1` for HOST1 and `appIdentity2` for HOST2.

16.5.6 Configuring the Managed WebLogic Servers to Use Custom Keystores

Follow these steps to configure the identity and trust keystores for each Managed Server:

1. Log in to Oracle WebLogic Server Administration Console at the URL listed in Section 31.2, "About Identity and Access Management Console URLs"
2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

   The Summary of Servers page appears.
5. Click the name of the server for which you want to configure the identity and trust keystores. The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. Click **Change** next to the Keystores label. On the Change page, change the keystrokes to **Custom Identity** and **Custom Trust**, and click **Save**.
8. In the Identity section, define attributes for the identity keystore:
   - **Custom Identity Keystore:** The fully qualified path to the identity keystore:

SHARED_CONFIG_DIR/keystores/appIdentityKeyStore.jks

- **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
- **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in Section 16.5.3, "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:

     SHARED_CONFIG_DIR/keystores/appTrustKeyStore.jks

   - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
   - **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in Section 16.5.3, "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_oim1`, use `appIdentity-OIMHOST1.example.com`
    - For `ADMINSERVER`, use `appIdentity-IGDADMINVHN.example.com`

    In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 16.5.2, "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 31.1, "Starting and Stopping Enterprise Deployment Components"

16.5.7 Changing the Host Name Verification Setting for the Managed Servers

Once the previous steps have been performed, set host name verification for the affected Managed Servers to `BEA Hostname Verifier`. To do this, perform the following steps:

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 appears.
5. Select the Managed Server in the **Names** column of the table.

   The settings page for the server appears.
6. Open the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `BEA Hostname Verifier`.
9. Select **Use JSEE SSL**.

   Note: This value must be selected after applying the mandatory WebLogic patches.
10. Click **Save**.
11. Click **Activate Changes**.

17

Configuring Oracle Access Management

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.

Access Manager consists of several components, including OAM Server, Oracle Access Management Console, and WebGates. The OAM Server includes all the components necessary to restrict access to enterprise resources. The Oracle Access Management Console is the administrative console to Access Manager. WebGates are web server agents that act as the actual enforcement points for Access Manager.

When you created the domain IAMAccessDomain in Chapter 15, "Creating Domains for an Enterprise Deployment", you created the domain with all of the Oracle Access Management components. This chapter explains how to configure Oracle Access Management after the domain creation.

This chapter includes the following topics:

17.1 About Domain URLs

After you complete this chapter, the following URL will be available:

Table 17–1 OAM URLs Prior to Web Tier Integration

Component	URLs	User
OAM Console	`http://iadadminvhn.example.com:7001`	weblogic

Table 17–1 (Cont.) OAM URLs Prior to Web Tier Integration

Component	URLs	User
Access Console	`http://oamhost1.example.com:14150/access`	weblogic

After you complete this chapter, the following URL will be available:

Table 17–2 OAM URLs After Web Tier Integration

Component	URLs	User	SSO User
OAM Console	`http://IADADMIN.example.com/oamconsole`	weblogic	oamadmin
Access Console	`http://IADADMIN.example.com/access`	weblogic	oamadmin

17.2 Post-Installation Tasks

This section describes tasks to be completed after Installing Oracle Access Manager.

This section contains the following topics:

- Section 17.2.1, "Setting the Front End URL for the Administration Console"
- Section 17.2.2, "Removing IDM Domain Agent"
- Section 17.2.3, "Configuring and Integrating with LDAP"
- Section 17.2.4, "Updating WebGate Agents"
- Section 17.2.5, "Updating Host Identifiers"
- Section 17.2.6, "Adding Missing Policies to OAM"

17.2.1 Setting the Front End URL for the Administration Console

Oracle WebLogic Server Administration Console tracks changes 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:

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 **Clusters** to open the Summary of Servers page.
5. Select **cluster_ama** in the **Names** column of the table.

   The Settings page appears.
6. Click the **Configuration** tab.
7. Click the **HTTP** tab.

8. Set the **Front End Host and Front End HTTP PORT** fields to your load balancer address, as shown below.

Table 17–3 Front End URL Information

Domain	Front End Host	Front End HTTP Port
IAMAccessDomain	iadadmin.example.com	80

9. Save and activate the changes.

17.2.2 Removing IDM Domain Agent

By default, the IDMDomainAgent provides single sign-on capability for administration consoles. In enterprise deployments, WebGate handles single sign-on, so you must remove the IDMDomainAgent.

To remove the IDMDomainAgent:

Log in to the WebLogic console at the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

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 Administration Server and ALL running Managed Servers, as described in Section 31.1.5.1, "Starting and Stopping a WebLogic Administration Server".

17.2.3 Configuring and Integrating with LDAP

This section describes how to configure and integrate Oracle Access Manager with LDAP.

This section contains the following topics:

- Section 17.2.3.1, "Setting a Global Passphrase"
- Section 17.2.3.2, "Configuring Access Manager to use the LDAP Directory"
- Section 17.2.3.3, "Adding LDAP Groups to WebLogic Administrators"

17.2.3.1 Setting a Global Passphrase

By default, Access Manager is configured to use the Open security model. If you plan to change this mode using `idmConfigTool`, you must set a global passphrase. Although you need not set the global passphrase and the Web gate access password to be the same, Oracle recommends doing so.

To set a global passphrase:

1. Log in to the OAM console at the URL listed in Section 31.2, "About Identity and Access Management Console URLs" as the WebLogic Administration user.
2. Click the **Configuration** tab.
3. Select **View**, and then **Access Manager** from the **Settings** launch pad.
4. If you are going to change the security mode to `Simple`, supply a global passphrase.
5. Click **Apply**.

17.2.3.2 Configuring Access Manager to use the LDAP Directory

Now that the initial installation is done and the security model set, you must now associate Access Manager and your LDAP directory. In this release, the following LDAP directories are supported:

- Oracle Unified Directory (OUD)
- Oracle Internet Directory (OID)
- Microsoft Active Directory (AD)

To associate Access Manager and your LDAP directory, perform the following tasks:

- Section 17.2.3.2.1, "Creating a Configuration File"
- Section 17.2.3.2.2, "Integrating Access Manager and LDAP Using the idmConfigTool"
- Section 17.2.3.2.3, "Validating the OAM LDAP Configuration"

17.2.3.2.1 Creating a Configuration File Configuring Oracle Access Management to use LDAP requires running the `idmConfigTool` utility. Therefore, you must create a configuration file called `oam.props` to use during the configuration. The contents of this file will be the same as the Configuration file created in Section 13.2, "Creating a Configuration File" with the following additions:

```
# Miscellaneous Properties
SPLIT_DOMAIN: true
# OAM Properties
OAM11G_IDSTORE_NAME: OAMIDSTORE
PRIMARY_OAM_SERVERS: oamhost1.example.com:5575,oamhost2.example.com:5575
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_OIM_WEBGATE_PASSWD: Password
COOKIE_DOMAIN: .example.com
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_WG_DENY_ON_NOT_PROTECTED: true
OAM11G_IDM_DOMAIN_OHS_HOST: login.example.com
OAM11G_IDM_DOMAIN_OHS_PORT: 443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL: https
OAM11G_SERVER_LBR_HOST: login.example.com
OAM11G_SERVER_LBR_PORT: 443
OAM11G_SERVER_LBR_PROTOCOL: https
OAM11G_OAM_SERVER_TRANSFER_MODE: simple
OAM_TRANSFER_MODE: simple
OAM11G_SSO_ONLY_FLAG: false
OAM11G_IMPERSONATION_FLAG: false
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_OIM_OHS_URL: https://prov.example.com:443/
```

```
# WebLogic Properties
WLSHOST: IADADMINVHN.example.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: IDM Administrators
```

OAM Property Descriptions:

- **OAM11G_IDSTORE_NAME** is the name you wish to assign to the ID store in OAM. This is an optional parameter.
- **PRIMARY_OAM_SERVERS** a comma-separated list of all of the OAM managed servers that are in the deployment. The format of this is Server Running the OAM Managed Server: OAM Proxy port. Note the proxy port used is not the OAM managed server listen port. The OAM Proxy port can be found in the worksheet (OAM_PROXY_PORT)
- **WEBGATE_TYPE** The type of webgate profile to create. This should always be `ohsWebgate11g`
- **ACCESS_GATE_ID** is the name of the Webgate Agent to create.
- **OAM11G_OIM_WEBGATE_PASSWD** is the password you wish to assign to the webgate agent you will be creating.
- **COOKIE_DOMAIN** is the domain you wish to associate the OAM cookie with this is normally the same as the *IDSTORE_SEARCH_BASE* in domain format. The search base can be found in the worksheet (REALM_DN).
- **COOKIE_EXPIRY_INTERVAL** the amount of time before a cookie is expired.
- **OAM11G_WG_DENY_ON_NOT_PROTECTED** this should always be set to true. It ensures that any attempt to access a resource not explicitly stated in the OAM Resource list will be rejected.
- **OAM11G_IDM_DOMAIN_OHS_HOST** this is the name of the Oracle HTTP Server (OHS) server which fronts the IAMAccessDomain. In the case of an enterprise deployment this will be the load balancer name.
- **OAM11G_IDM_DOMAIN_OHS_PORT** this is the port on which the OHS server fronting the IAMAccessDomain listens. In the case of an Enterprise Deployment, this will be the load balancer port. This is the IAD_HTTPS_PORT in the worksheet.
- **OAM11G_IDM_DOMAIN_OHS_PROTOCOL** this determines which process is being used when accessing the OHS server fronting the IAMAccessDomain.In the case of an Enterprise Deployment this will be the load balancer protocol. In the Enterprise Deployment Blueprint SSL is terminated at the load balancer. But the URL will always have the HTTPS prefix, so this value should be set to `https`.
- **OAM11G_SERVER_LBR_HOST** this is the name of the virtual host configured on the load balancer for logging in. This is usually the same as **OAM11G_IDM_DOMAIN_OHS_HOST**.
- **OAM11G_SERVER_LBR_PORT** this is the port of the virtual host configured on the load balancer for logging in. This is usually the same as **OAM11G_IDM_DOMAIN_OHS_PORT**.
- **OAM11G_SERVER_LBR_PROTOCOL** this is the protocol of the virtual host configured on the load balancer for logging in. This is usually the same as **OAM11G_IDM_DOMAIN_OHS_PROTOCOL**.

- **OAM11G_OAM_SERVER_TRANSPORT_MODE** this is the type of OAM security transport to be used. This should be `Simple` for all platforms, except for AIX where it should be `Open`. You can specify `cert` if extra security is required. If you wish to use `cert`, refer to the Oracle Access Manager documentation for how to configure this.
- **OAM_TRANSFER_MODE** this is the type of OAM security transport to be used. This should be the same as **OAM11G_OAM_SERVER_TRANSPORT_MODE**
- **OAM11G_SSO_ONLY_FLAG** this is used to determine whether authentication mode is going to be used. For Enterprise Deployments this should be set to `false`.
- **OAM11G_IMPERSONATION_FLAG** determines whether OAM be configured for impersonation. Impersonation is typically used in help desk type applications where a support user "impersonates" and actual user for the purposes of providing support.
- **OAM11G_IDM_DOMAIN_LOGOUT_URLS** is a list of URLs that various products can invoke for the purposes of logging out.
- **OAM11G_OIM_INTEGRATION_REQ** specifies whether Oracle Identity Manager is integrated with Oracle Access Manager. If you are creating a topology containing both Oracle Access Manager and Oracle Identity Manager, this parameter should be set to `true`. Otherwise set it to `false`.

  If, at a later date, you decide to add Oracle Identity Manager into your topology, rerun the OAM configuration with this flag set to `true`
- **OAM11G_OIM_OHS_URL** this is used when OAM and OIM are being integrated. This is the OIM URL to which OAM directs requests. This url is made up of the following values from the worksheet:

  `https://prov.example.com:`*`IAG_HTTPS_PORT`*`/`
- **WLS_HOST**: is the Admin Server listen address. For OAM configuration, this will be `IADADMINVHN.example.com`
- **WLS_PORT**: is the Admin Server listen port. This is the IAD_WLS_PORT in the worksheet.
- **WLS_ADMIN** the user used to connect to the Admin Server
- **SPLIT_DOMAIN** is used when OAM and OIM are in different domains. This should always be set to `true`.

17.2.3.2.2 Integrating Access Manager and LDAP Using the idmConfigTool

This section describes how to integrate Oracle Access Manager and LDAP using the `idmConfigTool`.

Perform the following tasks on OAMHOST1:

1. Set the environment variables MW_HOME, JAVA_HOME and ORACLE_HOME.

   ```
   Set ORACLE_HOME to IAD_ORACLE_HOME.
   MW_HOME to IAD_MW_HOME
   ```

2. Run the idmConfigTool utility to perform the integration.

   The syntax of the command on Linux is:

   ```
   cd IAD_ORACLE_HOME/idmtools/bin
   idmConfigTool.sh -configOAM input_file=configfile
   ```

For example:

```
idmConfigTool.sh -configOAM 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. You are also asked to specify the passwords you want to assign to these accounts:

- IDSTORE_PWD_OAMSOFTWAREUSER
- IDSTORE_PWD_IADADMINUSER
- OAM11G_IDM_DOMAIN_WEBGATE_PASSWD

3. 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.
4. Restart WebLogic Administration console, WLS_OAM1, WLS_OAM2, WLS_AMA1, WLS_AMA2.

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 following directory:

IAD_ASERVER_HOME/output/Webgate_IDM_11g

You need these when you install the WebGate software.

- cwallet.sso
- ObAccessClient.xml
- password.xml
- aaa_cert.pem
- aaa_key.pem

Note: If the `wls_ama` servers were running when `configOAM` was run, then the `WebGate_IDM` artifacts may have been created in *IAD_MSERVER_HOME*/output. If this is the case, move them back to *IAD_ASERVER_HOME*/output.

17.2.3.2.3 Validating the OAM LDAP Configuration

To validate that this has completed correctly:

1. Access the OAM console using the following URL:

   ```
   http://iadadmin.example.com/oamconsole
   ```

2. Log in as the Access Manager administration user you created when you prepared the ID Store. For example `oamadmin`.
3. Click **Agents Launch pad** from the Application Security screen.
4. When the Search SSO Agents screen appears, click **Search**.
5. You should see the Web Gate agent Webgate_IDM and Webgate_IDM_11g.

17.2.3.3 Adding LDAP Groups to WebLogic Administrators

Access Manager requires access to MBeans stored within the administration server. In order for Access Manager to invoke these Mbeans, users in the OAM Administrators group must have WebLogic Administration rights.

When Single Sign-on is implemented, provide the LDAP group IDM Administrators with WebLogic administration rights, so that you can log in using one of these accounts and perform WebLogic administrative actions.

To add the LDAP Groups `OAMAdministrators` and `IDM Administrators` to the 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.
6. Click the **Roles** link to go to the Global Roles page.
7. On the Global Roles page, click the **Admin** role to go to the Edit Global Roles page.
8. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.
9. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.
10. On the Edit Arguments Page, Specify **OAMAdministrators** in the **Group Argument** field and click **Add**.
11. Repeat for the Group **IDM Administrators**.
12. Click **Finish** to return to the Edit Global Roles page.
13. The **Role Conditions** table now shows the groups **OAMAdministrators and IDM Administrators** as role conditions.
14. Click **Save** to finish adding the Admin role to the OAMAdministrators and IDM Administrators Groups.

17.2.4 Updating WebGate Agents

When the `idmConfigTool` is run, it changes the default OAM security model and creates two new WebGate profiles. However, it does not change the existing WebGate profiles to the new security model. After running the `idmConfigTool`, you must update any WebGate agents that previously existed. This involves the following steps:

- Change the security mode to match that of the OAM servers. Failure to do so will result in a security mismatch error.
- When WebGates are created at first install, they are unaware that a highly available (HA) installation is performed. After enabling HA, you must ensure that all of the OAM servers are included in the agent configuration, to ensure system continuity.
- When WebGates are created at first install, they are unaware that a highly available (HA) install is performed. You must check that any logout URLs are redirected to the hardware load balancer than one of the local OAM servers.

- A WebGate agent called **IAMSuiteAgent** is created out of the box. This is created without any password protection and needs to have one added.

To perform these actions, complete the following steps:

1. Log in to the OAM Console as the Access Management administrator user. For example, use the following URL:

   `http://iadadmin.example.com:7101/oamconsole`

2. Click **Agents Launch** pad on the Application Security screen.
3. Ensure that the **WebGates** tab is selected.
4. Click **Search**.
5. Click an Agent, for example: **IAMSuiteAgent**.
6. Set the Security value to the same value defined to **OAM Transfer Mode** on the Access Manager Configuration screen during response file creation.

   The default setting is Open for AIX deployments and Simple for all others.

   If you have changed the OAM security model using the `idmConfigTool`, change the security model used by any existing Webgates to reflect this change.

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

   Assign an Access Client Password, such as the **Common IAM Password** (*COMMON_IDM_PASSWORD*) you used during the response file creation or an Access Manager-specific password, if you have set one.
9. Set **Maximum Number of Connections** to 20. This is the total maximum number of connections for the primary servers, which is 10 x WLS_OAM1 connections plus 10 x WLS_OAM2 connections.
10. If you see the following in the **User Defined Parameters**:

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

    Change it to:

    ```
    logoutRedirectUrl=https://login.example.com/oam/server/logout
    ```

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

17.2.5 Updating Host Identifiers

When you access your domain you enter using different load balancer entry points. Each of these entry points (virtual hosts) need to be added to the Policy list. This ensures that if you request access to a resource using `login.example.com` OR `prov.example.com`, you have access to the same set of policy rules.

1. Access the OAM console.
2. Log in as the Access Manager administration user you created when you prepared the ID Store. For example `oamadmin`.

3. Select **Launch Pad** if not already displayed.
4. Click on **Host Identifiers** under **Access Manager**.
5. Click **Search**.
6. Click on **IAMSuiteAgent**.
7. Click **+** in the operations box.
8. Enter the following information.

Table 17–4 Host Name Port Values

Host Name	Port
`iadadmin.example.com`	80
`igdadmin.example.com`	80
`prov.example.com`	443
`login.example.com`	443

9. Click **Apply**.

17.2.6 Adding Missing Policies to OAM

If you are using Oracle Mobile Security Suite (OMSS) or OIM, you manually add the policies listed in Table 17–5 to OAM.

Table 17–5 OAM Policy Information

Product	Resource Type	Host Identifier	Resource URL	Protection Level	Authentication Policy	Authorization Policy
ALL	HTTP	IAMSuiteAgent	`/consolehelp/**`	Excluded		
OMSS	HTTP	IAMSuiteAgent	`/gms-rest/**`	Excluded		
	HTTP	IAMSuiteAgent	`/msm-mgmt/**`	Excluded		
	HTTP	IAMSuiteAgent	`/ecp/**`	Excluded		
	HTTP	IAMSuiteAgent	`/msm/**`	Excluded		
	HTTP	IAMSuiteAgent	`/msmconsole/**`	Protected	Protected Higher Level Policy	Protected Resource Policy
	HTTP	IAMSuiteAgent	`/xmlpserver/**`	Excluded		

To add these policies:

1. Login to the OAM Console using the user `oamadmin`.
2. From the Launchpad click **Application Domains** in the **Access Manager** section.
3. Click **Search** on the Search page.

A list of Application domains appears.

4. Click the domain **IAM Suite**.
5. Click the **Resources** Tab.
6. Click **Create**.
7. Enter information according to Table 17–5.
8. Click **Apply**.

17.3 Validating Access Manager

You can validate Access Manager by using the `oamtest` tool. To do this, perform the following steps:

1. Ensure that wls_oam managed server is up and running.
2. Ensure that JAVA_HOME is set in your environment by adding *JAVA_HOME*`/bin` to your path. For example:

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

3. Change the directory to the following:

   ```
   IAD_ORACLE_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**: `OAMHOST1.example.com`
   - **Port**: `5575` (*OAM_PROXY_PORT*)
   - **Agent ID**: `Webgate_IDM_11g`
   - **Agent Password**: `webgate password`

   Note: If you configured `simple` mode, select **Simple** and provide the global passphrase.

   Click **Connect**.

   In the status window you see: `response] Connected to primary access server`.
6. In the Protected Resource URI section, enter the following information:
   - **Scheme**: http
   - **Host**: `iadadmin.example.com`
   - **Port**: `80` (IAD_HTTP_PORT)
   - **Resource**: `/oamconsole`

   Click **Validate**.

   In the status window 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: `[request] [authenticate] yes`
- Click **Authorize**.
- In the status window you see. `[request] [authorize] yes`

17.4 Creating Access Manager Key Store

If you are integrating other components, such as Oracle Identity Manager with Access Manager and Access Manager is using the simple security transport model, you must generate a keystore that can be used with those components.

Access Manager 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 as follows

The following example will add the Trust Store to the system generated keystore and place it into a common location.

1. Create a directory for the keystore to reside, if not created already. For example, *SHARED_CONFIG_DIR*/keystores.
2. Copy the system generated keystore to this location and give it a unique name using the following command:

   cp *IAD_ASERVER_HOME*/output/webgate-ssl/oamclient-keystore.jks *SHARED_CONFIG_DIR*/keystores/ssoKeystore.jks
3. To add the trust store to the keystore file you first add a dummy entry to create the keystore file and 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:

   PATH=$IAD_MW_HOME/jdk:$PATH

   The certificate resides in the file cacert.der, which is located in the following directory:

   IAD_MW_HOME/iam/oam/server/config

   Set JAVA_HOME to *JAVA_HOME* and add JAVA_HOME/bin to your PATH.

   Execute the following command to import a PEM/DER format CA certificate into the trust store:

   keytool -importcert -file *IAD_ORACLE_HOME*/oam/server/config/cacert.der -trustcacerts -keystore *SHARED_CONFIG_DIR*/keystores/ssoKeystore.jks -storetype JKS

   Enter keystore password when prompted.

   The password is the common password you used for the global passphrase.

   Note: The files ssoKeystore.jks is required when you integrate Access Manager running in Simple mode with Oracle Identity Management or Adaptive Access Manager.

17.5 Updating Idle Timeout Value

The default timeout value set in Access Manager is often too long and can cause issues such as, not logging a session out after that session has timed out. Therefore, it is recommended that this value is reduced to 15 minutes.

To update the idle timeout value:

1. Log in to the OAM Console at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. Log in as the Access Manager administrator user you created during response file creation. For example:

   `oamadmin`
3. Click **Configuration**.
4. Select **Common Settings** under **Settings**.
5. Change **Idle Time out (minutes)** to `15`.
6. Click **Apply**.

17.6 Updating the ESSO IDS Repository

The ESSO Identity Store Repository is created by default as ssl enabled. If the LDAP connection is not SSL enabled, update the IDS repository to uncheck the ssl flag by doing the following:

1. Log in to the OAM Console at the URL listed in Section 31.2, "About Identity and Access Management Console URLs".
2. Log in as the Access Manager administrator user you created during response file creation. For example: `oamadmin`
3. Click **Configuration**.
4. Click **User Identity Stores**.
5. Select **ESSOIDSRepository** under the section **IDS Repositories**, and click **Edit**.
6. Uncheck the flag **SSL**.
7. Click **Save**.
8. Click **Apply** on the User Identity Stores page.

17.7 Enabling Exalogic Optimizations

This section describes post-deployment steps for Exalogic implementations.

This section includes the following topic:

- Section 17.7.1, "Enabling OAM Persistence Optimizations"

17.7.1 Enabling OAM Persistence Optimizations

You can speed up OAM persistence by enabling OAM Exalogic optimizations by adding a new parameter to the server start options for each OAM managed server.

To enable OPMS optimizations:

1. Log in to the WebLogic Console in the `IAMAccessDomain`.

See the Console URLs in Section 31.2, "About Identity and Access Management Console URLs.".

2. Navigate to **Environment**, and then **Servers**.
3. Click **Lock and Edit**.
4. Click on the server **WLS_OAM1**.
5. Click on the **Server Start** subtab.
6. Add the following to the Arguments field:

   ```
   -Doracle.oam.sme.elo=true
   ```

7. Click **Save**.
8. Repeat Steps 4-7 for the managed server `WLS_OAM2`.
9. Click **Activate Changes**.

17.8 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 information on database backups, refer to your database documentation.

To back up the installation to this point, back up the following:

- The Web tier
- The Access Manager database.
- The Administration Server domain directory
- The Managed Server domain directory
- The LDAP Directory
- The Keystores created

18

Configuring Oracle Mobile Security Services

This chapter describes how to configure Oracle Mobile Security Services (OMSS). Before performing any of the steps in this section, ensure that the latest Mobile Security Suite and Mobile Security Access Server Bundle Patches have been applied.

Oracle Mobile Security Services (OMSS) will be deployed when you configure Oracle Access Management. However, to use its functionality, you must configure OMSS.

This chapter includes the following topics:

18.1 Creating the Configuration Files

Create two properties files - `msm.props` and `msas.props`. The content of these files must be same as the file you created in Section 13.2, "Creating a Configuration File", with the following additional properties:

> **Note:** if your deployment is on Exalogic, you must provide the OTD fail-over group name for `IDSTORE_HOST` parameter. For non-Exalogic setups, provide the LBR entry point for `IDSTORE_HOST`.

- For `msm.props` file:

```
# OMSS Properties

OMSS_OMSM_IDSTORE_PROFILENAME: MSSProfile

OMSS_DOMAIN_LOCATION: /u01/oracle/config/domains/IAMAccessDomain

WLSHOST: iadadminvhn.example.com

WLSPORT: 7001
```

```
WLSADMIN: weblogic

WLSPASSWD: password

OMSS_SCEP_DYNAMIC_CHALLENGE_USER: msmadmin

OMSS_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators

OMSS_IDSTORE_ROLE_SECURITY_HELPDESK: MSMHelpDesk

OMSS_MSAS_SERVER_HOST: msas.example.com

OMSS_MSAS_SERVER_PORT: 9002

OAM_SERVER_URL: http://iadinternal.example.com:7777

OMSS_OMSM_SERVER_NAME: wls_msm1,wls_msm2

OMSS_OAM_POLICY_MGR_SERVER_NAME: wls_ama1,wls_ama2

OMSS_OMSM_SERVER_HOST:OAMHOST1.example.com,OAMHOST2.example.com

OMSS_OMSM_FRONT_END_URL: http://iadinternal.example.com:7777

OMSS_JDBC_URL: jdbc:oracle:thin:@(DESCRIPTION =
(ADDRESS=(PROTOCOL=TCP)(HOST=iaddb-scan.example.com)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=iadedg.example.com)))

OMSS_OMSM_SCHEMA_USER: EDGIAD_OMSM

OMSS_GATEWAY_INSTANCE_ID: EDGMSAS
```

- For `msas.props` file:

```
# OMSS Properties

OMSS_OMSM_IDSTORE_PROFILENAME: MSSProfile

WLSHOST: iadadminvhn.example.com

WLSPORT: 7001

WLSADMIN: weblogic

WLSPASSWD: password

OMSS_DOMAIN_LOCATION: /u01/oracle/config/domains/IAMAccessDomain

OMSS_SCEP_DYNAMIC_CHALLENGE_USER: msmadmin

OMSS_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators

OMSS_IDSTORE_ROLE_SECURITY_HELPDESK: MSMHelpDesk

OMSS_MSAS_SERVER_HOST: msas.example.com

OMSS_MSAS_SERVER_PORT: 9002

OAM_SERVER_URL=http://iadinternal.example.com:7777

OMSS_OMSM_SERVER_NAME: wls_msm1,wls_msm2

OMSS_OAM_POLICY_MGR_SERVER_NAME: wls_ama1,wls_ama2

OMSS_OMSM_FRONT_END_URL: http://iadinternal.example.com:7777

OMSS_JDBC_URL: jdbc:oracle:thin:@(DESCRIPTION =
(ADDRESS=(PROTOCOL=TCP)(HOST=iaddb-scan.example.com)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=iadedg.example.com)))

OMSS_OMSM_SCHEMA_USER: EDGIAD_OMSM
```

```
OMSS_OMSAS_IDSTORE_PROFILENAME: msas-profile

OMSS_GATEWAY_INSTANCE_ID: EDGMSAS
```

Description of the Properties:

Table 18–1 describes the properties used for Oracle Mobile Security Suite configuration.

Note: The value of the property `IDSTORE_DIRECTORYTYPE` must be specified in UPPERCASE.

The WebLogic Managed Server names in properties `OMSS_OMSM_SERVER_NAME` and `OMSS_OAM_POLICY_MGR_SERVER_NAME` must be specified in the same case as configured in WebLogic.

Table 18–1 Oracle Mobile Security Suite Configuration Properties

Property	Description
`OMSS_OMSM_IDSTORE_PROFILENAME`	Name of the identity store profile for Oracle Mobile Security Manager.
`OMSS_DOMAIN_LOCATION`	The absolute path to the Oracle Mobile Security Suite domain. This is the value of IAD_ASERVER_HOME from the worksheet.
`OMSS_SCEP_DYNAMIC_CHALLENGE_USER`	User account used for authentication.
`OMSS_IDSTORE_ROLE_SECURITY_ADMIN`	Name of the administrator group whose members have administrative privileges for Oracle Mobile Security Manager operations. This group is used to allow access to the Oracle Mobile Security Manager features on the Policy Manager Console. This should be set to the same value that you provided for `OAM11G_IDSTORE_ROLE_SECURITY_ADMIN` property in the Oracle Access Manager configuration properties file.
`OMSS_IDSTORE_ROLE_SECURITY_HELPDESK`	Name of the Oracle Mobile Security Manager helpdesk group whose members get helpdesk privileges for Oracle Mobile Security Manager operations. This group is used to allow access to the Security Help Desk privileges on the Policy Manager Console.
`OMSS_MSAS_SERVER_HOST`	The host name for Oracle Mobile Security Access Server. For example, `oamhost1.example.com` and `oamhost2.example.com`. If the Mobile Security Access Server instance is behind a load balancer, provide the host name of the load balancer.
`OMSS_MSAS_SERVER_PORT`	The SSL port where the Oracle Mobile Security Access Server instance will be running. This is the value of MSAS_PORT from the worksheet. If the Mobile Security Access Server instance is behind a load balancer, provide the port number of the load balancer.
`OAM_SERVER_URL`	This is the internal link for OAM internal calls. For example: http://iadinternal.example.com:7777
`OMSS_OMSM_SERVER_NAME`	A comma-separated list of Mobile Security Manager Managed Server names. For example, `wls_msm1,wls_msm2`.

Table 18–1 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
OMSS_OAM_POLICY_MGR_SERVER_NAME	A comma-separated list of Policy Manager Managed Server names. For example, wls_ama1,wls_ama2.
OMSS_OMSM_SERVER_HOST	A comma-separated list of host names hosting the Oracle Mobile Security Manager Managed Servers. For example, OAMHOST1.example.com, OAMHOST2.example.com.
OMSS_OMSM_FRONT_END_URL	The URL of the load balancer which routes requests to the Mobile Security Manager Managed Servers. For example: http://igdinternal.example.com:7777
OMSS_JDBC_URL	The JDBC URL to the Oracle Mobile Security Manager database repository, in the following format, where *db_host* is the host name of the machine on which the database resides, *port* is the listener port of the database, and *service_name* is the service name identified for the database: jdbc:oracle:thin:@*db_host*:port/*service_name*
OMSS_OMSM_SCHEMA_USER	The user name for the Oracle Mobile Security Manager schema, which consists of the prefix that was configured for the repository in RCU followed by _OMSM. For example, EDGIAD_OMSM.
OMSS_GATEWAY_INSTANCE_ID	The name of the Oracle Mobile Security Access Server gateway instance. The gateway instance ID must be the same as the instance ID you use when you configure Oracle Mobile Security Access Server. This property is only required when you are running the idmConfigTool -configOMSS mode=OMSAS command after you have configured your Oracle Mobile Security Access Server instance. This property should not be set when you are running the idmConfigTool for configuring Oracle Mobile Security Manager.
OMSS_OMSAS_IDSTORE_PROFILENAME	Name of the identity store profile for Oracle Mobile Security Access Server. This property is only required for running the idmConfigTool -configOMSS mode=OMSAS command after you have configured your Oracle Mobile Security Access Server instance. This property should not be set when you are running the idmConfigTool for configuring Oracle Mobile Security Manager.

Oracle Mobile Security Manager can send notifications such as the number of unread e-mails. To enable this, you must provide the exchange server and email server details using the properties described in Table 18–2. These properties are optional and can be provided after the configuration, if required.

Table 18–2 Optional Properties for Oracle Mobile Security Suite Configuration

Property	Description
OMSS_EXCHANGE_SERVER_URL	The URL of the Exchange server that Oracle Mobile Security Suite will connect to.
OMSS_EXCHANGE_LISTENER_URL	The listener URL of the Exchange server that Oracle Mobile Security Suite will connect to.
OMSS_EXCHANGE_DOMAIN_NAME	The domain name of the Exchange server that Oracle Mobile Security Suite will connect to.
OMSS_EXCHANGE_ADMIN_USER	The administrative user name of the Exchange server that Oracle Mobile Security Suite will connect to.
OMSS_EXCHANGE_ADMIN_PASSWORD	The password of the Exchange Server administrator.
OMSS_EXCHANGE_SERVER_VERSION	The version number of the Exchange server that Oracle Mobile Security Suite will connect to.
OMSS_EMAIL_ADMIN_USER	The Email address of the Oracle Mobile Security Suite administrator.
OMSS_EMAIL_ADMIN_PASSWORD	The password of the Oracle Mobile Security Suite administrator's Email address.
OMSS_SMTP_HOST	The host name of the SMTP server that Oracle Mobile Security Manager will use to send Email invites to users.
OMSS_SMTP_PORT	The port number of the SMTP server that Oracle Mobile Security Manager will use to send Email invites to users.
OMSS_APPLE_CACERT_FILE	The location of Apple root CA. Required during iOS device enrollment in Oracle Mobile Security Suite.
OMSS_APNS_FILE	The full path and file name of the Apple Push Notification Service (APNs) keystore file, which is used to establish secure connection to Apple server and to send notifications. This should be the same location on all hosts. For example, *SHARED_CONFIG_DIR*/keystores/ APNS.p12
OMSS_APNS_KEYSTORE_TYPE	The type of keystore used for the Apple Push Notification Service (APNs) keystore file (OMSS_APNS_FILE). The valid keystore types are JKS or PKCS12. The default value is JKS.
OMSS_GCM_API_KEY	The API key value for Google Cloud Messaging (GCM) notification.
OMSS_GCM_SENDER_ID	The Google Cloud Messaging (GCM) notification sender ID.

18.2 Configuring Oracle Mobile Security Manager

Configure Oracle Mobile Security Manager (MSM) using the idmConfig tool. To do this, complete the following steps on OAMHOST1:

1. Set the following environment variables:
   - Set MW_HOME to *IAD_MW_HOME*
   - Set JAVA_HOME to *JAVA_HOME*
   - Set ORACLE_HOME to *IAD_ORACLE_HOME*
   - Set WL_HOME to *IAD_MW_HOME*/wlserver_10.3

2. Change directory to the *IAD_ORACLE_HOME*/idmtools/bin directory using the following command:

   ```
   cd IAD_ORACLE_HOME/idmtools/bin
   ```

3. Run the following command:

   ```
   idmConfigTool.sh -configOMSS mode=OMSM input_file=configfile
   ```

   In this command, *configfile* is the full or relative path to the properties file (msm.props) you created in Creating the Configuration Files.

   For example:

   ```
   idmConfigTool.sh -configOMSS mode=OMSM input_file=msm.props
   ```

   When the command runs, you will be prompted to enter the password of the account that is used to connect to the identity store. It also prompts you to enter passwords for the following:

   - OMSS Keystore: Enter the password that will be assigned to the OMSS keystore when it is created.
   - SCEP Dynamic Challenge Password: Enter the password for the SCEP Dynamic Challenge user.
   - OMSM Schema User Password: Enter the password of the Oracle Mobile Security Manager schema (*prefix*_OMSM) created using RCU.

   The following is the sample command output:

   ```
   (1/8) MSM Configurations                                Success
   (2/8) Seeding User Notification Templates               Success
   (3/8) Seeding CSF Credentials                           Success
   (4/8) Configuring IDS Profile                           Success
   (5/8) Configuring OMSS Authentication Provider          Success
   (6/8) Creating MSM Keystores                            Success
   (7/8) Configuring MSM Server's SSL                      Success
   (8/8) OAM Console Integration                           Success
   ```

   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.

   This process creates objects in the domain. To make these objects visible, you must restart the Administration Server.

4. Pack the *IAMAccessDomain* on OAMHOST1 and unpack it on OAMHOST1 and OAMHOST2.

   To pack the *IAMAccessDomain*, run the following command on OAMHOST1 from the location *IAD_MW_HOME*/oracle_common/common/bin:

   ```
   ./pack.sh -managed=true -domain=IAD_ASERVER_HOME
   -template=domaintemplateMSM.jar -template_name=domain_template_MSM
   ```

Note: The `pack` command does not overwrite existing files. If the file name that you specify matches the name of an existing file in the specified folder, the `pack` command fails. You must use a different name for the template file for `pack` command and use the option `overwrite_domain=true` for the `unpack` command.

The `-overwrite_domain` option in the `unpack` command allows unpacking a Managed Server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the Managed Server domain directory, they must be restored after the `unpack` operation.

To unpack the *IAMAccessDomain*, run the following command on both OAMHOST1 and OAMHOST2 from the location *IAD_MW_HOME*`/oracle_common/common/bin`:

```
./unpack.sh -domain=IAD_MSERVER_HOME -template=domaintemplateMSM.jar
-app_dir=IAD_MSERVER_HOME/applications -overwrite_domain=true
```

Before you run the `unpack` command, ensure that you have write permissions on the *LOCAL_CONFIG_DIR*`/domains/` directory.

5. Restart the WebLogic Administration console, and start the following servers:
   - Oracle Access Manager Managed Servers (wls_oam1, wls_oam2)
   - Oracle Access Manager Policy Manager Managed Servers (wls_ama1, wls_ama2)
   - Oracle Mobile Security Manager Managed Servers (wls_msm1, wls_msm2)

   Note: If you are using OUD, just start the Administration Server at this stage.

18.3 Performing Additional Task for Oracle Unified Directory

If you are using Oracle Unified Directory (OUD) as the LDAP identity store and the group object class is groupOfUniqueNames, perform the following additional steps:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location *IAD_ORACLE_HOME*`/common/bin`:

   ```
   ./wlst.sh
   ```

2. Connect to the WebLogic Administration Server using the following command:

   ```
   connect(username='weblogic', password='wls_admin_password',
   url='t3://IADADMINVHN:IAD_WLS_PORT')
   ```

   For example:

   ```
   connect(username='weblogic', password='wls_admin_password',
   url='t3://iadadminvhn.example.com:7001')
   ```

3. Run the following WLST commands in the same order:
   - `edit()`
   - `startEdit()`

- `cd('/SecurityConfiguration/IAMAccessDomain/Realms/myrealm/AuthenticationProviders/OUDAuthenticator')`
- `cmo.setStaticMemberDNAttribute('uniquemember')`
- `cmo.setStaticGroupDNsfromMemberDNFilter('(&(uniquemember=%M)(objectclass=groupOfUniqueNames))')`
- `cmo.setStaticGroupObjectClass('groupOfUniqueNames')`
- `activate()`

4. Restart the WebLogic Administration Server and all the Managed Servers.

18.4 Verifying Oracle Mobile Security Manager Configuration

Verify the configuration of Oracle Mobile Security Manager and Access Manager by completing the following steps:

1. Ensure that the following servers are up and running:
   - Oracle WebLogic Administration Server
   - Oracle Access Manager Managed Servers (for example, wls_oam1)
   - Oracle Access Manager Policy Manager Managed Servers (for example, wls_ama1)
   - Oracle Mobile Security Manager Managed Server (for example, wls_msm1)
2. Log in to the Administration Console for Oracle Access Management using the following URL:

   `http://`*`iadadmin.example.com`*`/oamconsole`
3. Log in to the Access Console using the following URL:

   `http://`*`iadadmin.example.com`*`/access`
4. On the Policy Manager console (`http://`*`iadadmin.example.com`*`/access`), go to the **Configuration** tab.

   The Configuration Launch Pad opens.
5. On the Configuration Launch Pad, click **Available Services**.

   The Available Services page opens.
6. Ensure that the status of **Mobile Security Service** has a green check mark. If not, click **Enable Service** next to **Mobile Security Service** to enable the status of Mobile Security Service.
7. After enabling Mobile Security Service, log out of the Policy Manager Console and then log in again.
8. To access the Mobile Security Manager console pages, click **Mobile Security** at the top of the screen. The Mobile Security Launch Pad opens.

   Under **Mobile Security Manager**, click **View** to choose from the Mobile Security Manager console pages in the menu.
9. Access the resource `http://`*`iadinternal.example.com`*`:7777/msm-mgmt/scim/v1/endpoints`

   You should be prompted for a user name and password. Use the oamadmin username and password. The page should be displayed without errors.

18.5 Configuring MSAS Gateway Instances

You must have installed Oracle Mobile Security Access Server (MSAS) in Section 11.2.3, "Installing Oracle Mobile Security Access Server."

After you configure Oracle Mobile Security Manager, you must configure Oracle Mobile Security Access Server Gateway instances. Each instance must be configured exactly the same, with the same instance id, so that they can function as a cluster. While this can be done interactively, it is better to do so by using a property file, which can then be used to configure each instance.

To configure MSAS Gateway instances, complete the following steps:

1. Create a property file named `msas_instance.props` with the following properties:

   `MSM_URL`: `http://`*`iadinternal.example.com`*`:7777`

   `MSM_USER_NAME`: *`weblogic`*

   `MSAS_INSTANCE_ID`: *`EDGMSAS`*

   `MSAS_INSTANCE_ROOT_DIR`: *`LOCAL_CONFIG_DIR`*`/instances/`

   `MSAS_INSTANCE_SSL_PORT`: *`9002`*

   `MSAS_LBR_URL: https://`*`msas.example.com`*`:9002`

   `OAM_HOST`: *`iadadminvhn.example.com`*

   `OAM_PORT`: *`7001`*

   `OAM_USER_NAME`: *`oamadmin`*

   `OAM_PROTECT`: `/`

   `OAUTH_HOST`: *`login.example.com`*

   `OAUTH_PORT`: *`443`*

   `OAUTH_IS_SSL`: *`true`*

   `OAUTH_SP_ENDPOINT`: */oauthservice*

   `OAM_COOKIE_DOMAIN`: *`.example.com`*

   Table 18–3 describes the properties used for configuring MSAS Gateway instances.

Table 18–3 Properties for Configuring MSAS Gateway Instances

Property	Description
`MSM_URL`	The URL for the MSM server that you want this MSAS instance to be registered with. Enter the URL for the MSM server in the following format, where host is either the host name or the IP address of the MSM server and the port number is the listen port for the MSM server. `http://`*`host:port_number`* For example: `http://iadinternal.example.com:7777`
`MSM_USER_NAME`	The WebLogic Server Administrator username for the MSM domain.
`MSAS_INSTANCE_ID`	A unique name to identify the MSAS instance. It can be any string and must be consistent across instances. This must be same as the value of `OMSS_GATEWAY_INSTANCE_ID`.

Table 18–3 (Cont.) Properties for Configuring MSAS Gateway Instances

Property	Description
MSAS_INSTANCE_ROOT_DIR	Location where the instance configuration files will be created. For example: *LOCAL_CONFIG_DIR*/instances
MSAS_INSTANCE_PORT	The port that MSAS listens for requests on. This port is SSL enabled. This is the value of MSAS_PORT from the worksheet.
MSAS_LBR_URL	This is the load balancer entry point for Mobile Security Access Server. For example: https://*msas.example.com*:9002
OAM_HOST	The *IAMAccessDomain* Administration Server Virtual Host. For example: IADADMINVHN.example.com
OAM_PORT	The port that the *IAMAccessDomain* Administration Server uses. For example, 7001.
OAM_USER_NAME	The OAMAdmin account your created above.
OAM_PROTECT	The resource pattern for each protected application. For example: /myapp/login The pattern you enter is relative to the host and port of the Access Manager gateway. This entry must begin with a /. If you enter /, any requesting URL ending with / will be protected.
OAUTH_HOST	The OAUTH entry point in an Enterprise Deployment. This will be the load balancer name. For example: login.example.com
OAUTH_PORT	The port that OAM Managed Servers use in an Enterprise Deployment. This will be the load balancer port. For example: 443
OAUTH_IS_SSL	This property specifies where oauth is using the SSL or non SSL port. Valid values are true and false. In an Enterprise Deployment, this value must be true.
OAUTH_SP_ENDPOINT	The endpoint where you are accessing clients from the OAuth server. For example: /oauthservice

2. Configure the MSAS Gateway instance by running the following command from the location *MSAS_ORACLE_HOME*/omsas/bin, on WEBHOST1:

   ```
   ./configMSAS.sh -properties msas_instance.props
   ```

   When the command is run, you will be prompted for the following passwords:

- Mobile security manager password: This is the WebLogic Administrator password of the IAMAccessDomain.
- OAM Administrator Password: This is the Access Manager Administrator password.

When the configuration is completed, the MSAS instance is created in the directory *LOCAL_CONFIG_DIR*/instances/*gateway-id*, where the gateway-id is the value you provided in the property file. Validate that this directory exists.

3. Repeat this procedure on WEBHOST2.
4. Verify that the MSAS Gateway instance has been registered with MSM by performing the following steps:
   1. Log in to the access console as the oamadmin user.
   2. On the launch pad, click **Mobile Security**.
   3. Click **Environments** in the **Mobile Security Access Server** section. The MSAS instances are shown.

18.6 Integrating MSAS with the Identity Store

To integrate the MSAS with the identity store, complete the following steps on OAMHOST1:

1. Set the following environment variables:
   - Set MW_HOME to *IAD_MW_HOME*
   - Set JAVA_HOME to *JAVA_HOME*
   - Set ORACLE_HOME to *IAD_ORACLE_HOME*
   - Set WL_HOME to *IAD_MW_HOME*/wlserver_10.3
2. Change directory to the *IAD_ORACLE_HOME*/idmtools/bin directory using the following command:

   ```
   cd IAD_ORACLE_HOME/idmtools/bin
   ```

3. Run the following command:

   ```
   idmConfigTool.sh -configOMSS mode=OMSAS input_file=configfile
   ```

   In this command, *configfile* is the full or relative path to the properties file (msas.props) you created in Creating the Configuration Files.

   For example:

   ```
   idmConfigTool.sh -configOMSS mode=OMSAS input_file=msas.props
   ```

   When the command runs, you will be prompted to enter the password of the account that is used to connect to the identity store. It also prompts you to enter passwords for the following:

   - OMSS Keystore: Enter the password that will be assigned to the OMSS keystore when it is created.
   - SCEP Dynamic Challenge Password: Enter the password for the SCEP Dynamic Challenge user.
   - OMSM Schema User Password: Enter the password of the Oracle Mobile Security Manager schema (*prefix*_OMSM) created using RCU.

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.

This process creates objects in the domain. To make these objects visible, you must restart the Administration Server.

4. Pack the *IAMAccessDomain* on OAMHOST1 and unpack it on OAMHOST1 and OAMHOST2.

   To pack the *IAMAccessDomain*, run the following command on OAMHOST1 from the location *IAD_MW_HOME*/oracle_common/common/bin:

   ```
   ./pack.sh -managed=true -domain=IAD_ASERVER_HOME
   -template=domaintemplateMSAS.jar -template_name=domain_template_MSAS
   ```

   Note: The `pack` command does not overwrite existing files. If the file name that you specify matches the name of an existing file in the specified folder, the `pack` command fails. You must use a different name for the template file for `pack` command and use the option `overwrite_domain=true` for the `unpack` command.

   The `-overwrite_domain` option in the `unpack` command allows unpacking a Managed Server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the Managed Server domain directory, they must be restored after the `unpack` operation.

   To unpack the *IAMAccessDomain*, run the following command on both OAMHOST1 and OAMHOST2 from the location *IAD_MW_HOME*/oracle_common/common/bin:

   ```
   ./unpack.sh -domain=IAD_MSERVER_HOME -template=domaintemplateMSAS.jar
   -app_dir=IAD_MSERVER_HOME/applications -overwrite_domain=true
   ```

   Before you run the `unpack` command, ensure that you have write permissions on the *LOCAL_CONFIG_DIR*/domains/ directory.

5. Restart the WebLogic Administration console, and start the following servers:
   - Oracle Access Manager Managed Servers (wls_oam1, wls_oam2)
   - Oracle Access Manager Policy Manager Managed Servers (wls_ama1, wls_ama2)
   - Oracle Mobile Security Manager Managed Servers (wls_msm1, wls_msm2)

18.7 Adding Load Balancer Alias to MSAS Certificate

To prepare MSAS for high availability, you must update the MSAS Gateway SSL certificate with the load balancer alias. To do this, complete the following steps on OAMHOST1:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location *IAD_ORACLE_HOME*/common/bin:

   ```
   ./wlst.sh
   ```

2. Connect to the WebLogic Administration Server using the following command:

```
connect(username='wls_admin_username', password='wls_admin_password',
url='t3://IADADMINVHN.example.com:7001')
```

In this command, `7001` is the *IAD_WLS_PORT* from the worksheet.

3. Run the following commands:

   - `svc = getOpssService(name='KeyStoreService')`
   - `svc.exportKeyStore(appStripe='EDGMSAS',name='sslkeystore', password='password', aliases='EDGMSAS_msasidentity', keypasswords='keypassword', type='JKS',filepath='SHARED_CONFIG_DIR/keystores/EDGMSAS.jks')`

   In this command,

   EDGMSAS is the value you specified for the property `OMSS_GATEWAY_INSTANCE_ID`

   Password is the password of the WebLogic Administrator of the IAMAccessDomain

   keypassword is the password you wish to assign to the exported Keystore

4. Generate the new certificate request using the following command:

   ```
   keytool -keystore SHARED_CONFIG_DIR/keystores/EDGMSAS.jks -storepass
   password -alias EDGMSAS_msasidentity -certreq -file SHARED_CONFIG_
   DIR/keystores/msasidentity.csr -keypass keypassword
   ```

5. Sign the new certificate request with Certificate Authority key and add the load balancer's hostname in the certificate's Subject Alternate Name (SAN). Use the load balancer DNS extension, such as `msas.example.com`. To do this, run the following command:

   ```
   keytool -gencert -keystore IAD_ASERVER_
   HOME/config/fmwconfig/server-identity.jks -storepass password -alias ca
   -ext san=dns:msas.example.com -infile SHARED_CONFIG_
   DIR/keystores/msasidentity.csr -outfile SHARED_CONFIG_
   DIR/keystores/msasidentity.crt
   ```

6. Update the MSAS certificate on the server by completing the following steps:

   a. Export the root CA by running the following command:

      ```
      keytool -export -alias ca -file SHARED_CONFIG_DIR/keystores/ca.crt
      -keystore IAD_ASERVER_HOME/config/fmwconfig/server-identity.jks
      -storepass password
      ```

   b. Import the certificate into the EDGMSAS JKS keystore created in the previous step by running the following command:

      ```
      keytool -keystore SHARED_CONFIG_DIR/keystores/EDGMSAS.jks -import
      -file SHARED_CONFIG_DIR/keystores/ca.crt -alias ca -storepass
      password
      ```

      When this command is run, you will be prompted to trust the certificate. Enter **Yes**.

   c. Run the following command:

      ```
      keytool -keystore EDGMSAS.jks -import -file SHARED_CONFIG_
      DIR/keystores/msasidentity.crt -alias 'EDGMSAS_msasidentity'
      -storepass password
      ```

      In this command, `EDGMSAS` is the value you specified for the property `OMSS_GATEWAY_INSTANCE_ID`.

d. Import the new certificate into MSAS SSL keystore (KSS keystore) by running the following WLST commands:

```
svc = getOpssService(name='KeyStoreService')

svc.deleteKeyStoreEntry(appStripe='EDGMSAS',name='sslkeystore',pass
word='password', alias='EDGMSAS_msasidentity',
keypassword='keypassword')

svc.importKeyStore(appStripe='EDGMSAS', name='sslkeystore',
password='password', aliases='EDGMSAS_msasidentity',
keypasswords='keypassword', type='JKS',permission=true,
filepath='SHARED_CONFIG_DIR/keystores/EDGMSAS.jks')
```

18.8 Starting MSAS Instances

Start the MSAS instances on WEBHOST1 and WEBHOST2. To start the MSAS instances, run the following command:

```
MSAS_ORACLE_INSTANCE/bin/startServer.sh
```

The MSAS instances should start without error.

18.9 Verifying Oracle Mobile Security Suite Configuration

Verify that Mobile Security Suite is up and running by accessing the following URL:

```
https://msas.example.com:9002/msm/register/ios
```

You should be directed to a login page.

19

Configuring Oracle Identity Manager

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.

When you created the domain IAMGovernanceDomain in Chapter 15, "Creating Domains for an Enterprise Deployment", you created a domain containing the software parts for Oracle Identity Manager and Oracle Business Intelligence lite. Before you can use these products however you need to configure them. This chapter describes the procedures.

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 functionality:

- User Administration
- Workflow and Policy
- Password management
- Audit and Compliance Management
- Integration Solutions
- User Provisioning
- Organization and Role Management

About Domain URLs

Table 19–1 lists the Domain URLs and their corresponding components and SSO Users.

Table 19–1 Domain URL Details

Component	URL	SSO User
Self-service Console	`https://prov.example.com/identity`	xelsysadm
OIM Administration Console	`http://igdadmin.example.com/sysadmin`	xelsysadm

This chapter contains the following sections:

19.1 Configuring Oracle Coherence for Oracle SOA Suite

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in Oracle Identity and Access Management enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as Oracle Identity and Access Management enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

Note: An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the Oracle Identity and Access Management system from starting. The deployment framework must be properly customized for the network environment on which the system runs. Oracle recommends the configuration described in this section.

This section contains the following topics:

- Section 19.1.1, "Enabling Communication for Deployment Using Unicast Communication"
- Section 19.1.2, "Specifying the Host Name Used by Oracle Coherence"

19.1.1 Enabling Communication for Deployment Using Unicast Communication

Specify the nodes using the `tangosol.coherence.wka<n>` system property, where `<n>` is a number between 1 and 9. You can specify up to nine nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the tangosol.coherence.localhost system property. This local host name should be the virtual host name used by the SOA server as the listener addresses (OIMHOST1VHN2 and OIMHOST2VHN2). Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the **Arguments** field of the Oracle WebLogic Server Administration Console's Server **Start** tab.

Tip: To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

Note: OIMHOST1VHN2 is the virtual host name that maps to the virtual IP where WLS_SOA1 listening (in OIMHOST1). OIMHOST2VHN2 is the virtual host name that maps to the virtual IP where WLS_SOA2 is listening (in OIMHOST2).

19.1.2 Specifying the Host Name Used by Oracle Coherence

Use the Administration Console to specify a host name used by Oracle Coherence.

To add the host name used by Oracle Coherence

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.

   The Summary of Servers page appears.
4. Click the name of the server (WLS_SOA1 or WLS_SOA2, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit.**
6. Click the **Server Start** tab.
7. Enter the following for WLS_SOA1 and WLS_SOA2 into the **Arguments** field.

For WLS_SOA1, enter the following:

```
-Dtangosol.coherence.wka1=OIMHOST1VHN2
-Dtangosol.coherence.wka2=OIMHOST2VHN2
-Dtangosol.coherence.localhost=OIMHOST1VHN2
```

For WLS_SOA2, enter the following:

```
-Dtangosol.coherence.wka1=OIMHOST1VHN2
-Dtangosol.coherence.wka2=OIMHOST2VHN2
-Dtangosol.coherence.localhost=OIMHOST2VHN2
```

Note: There should be no breaks in lines between the different `-D` parameters. The parameters must be separated by a space character. Do not copy or paste the text to the arguments text field in the Administration Console. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included in the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the `-Dtangosol.coherence.wkan.port` and -Dtangosol.coherence.localport startup parameters. For example: WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=OIMHOST1VHN2
-Dtangosol.coherence.wka2=OIMHOST2VHN2
-Dtangosol.coherence.localhost=OIMHOST1VHN2
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=OIMHOST1VHN2
-Dtangosol.coherence.wka2=OIMHOST2VHN2
-Dtangosol.coherence.localhost=OIMHOST2VHN2
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

---

8. Click **Save and Activate Changes**.
9. Restart the WebLogic administration server
10. Start the SOA managed servers `wls_soa1` and `wls_soa2`.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

19.2 Configuring Oracle Identity Manager

You must configure the Oracle Identity Manager server instance before you can start the Oracle Identity Manager Managed Servers. For a consolidated topology, this is performed on IAMHOST2. For a distributed topology, this is performed on OIMHOST1. 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.
- SOA Managed 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.

To configure Oracle Identity Manager:

1. Start the Configuration Wizard by running the following command from the location *IGD_ORACLE_HOME*/bin/:

   ```
   ./config.sh
   ```

2. On the Welcome screen, click **Next**
3. On the Components to Configure screen, Select **OIM Server**.

   Click **Next**.
4. On the Database screen, provide the following values:
   - **Connect String**: The connect string for the Oracle Identity Manager database:

     ```
     igddb-scan.example.com:1521:igdedg1^igddb-scan.example.com:1521:igd
     edg2@igdedg.example.com
     ```

   - **OIM Schema User Name**: `edgigd_oim`
   - **OIM Schema password**: *password*
   - **MDS Schema User Name**: `edgigd_mds`
   - **MDS Schema Password**: *password*

   Click **Next**.
5. 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://IGDADMINVHN.example.com:7101
     ```

Where 7101 is the *IGD_WLS_PORT* from the worksheet.

- **UserName**: `weblogic`
- **Password**: Password for the `weblogic` user

Click **Next**.

6. 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. Best practice is to use the same password that you assigned to the user xelsysadm in preparing the Identity Store
   - **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://igdinternal.example.com:7777
     ```

   - **OIM External FrontEnd URL**:

     ```
     https://prov.example.com:IGD_HTTPS_PORT
     ```

   - **Key Store Password**: Key store password. The password must have an uppercase letter and a number.
   - **Enable OIM for Suite Integration**: Selected.

     Select this option if you plan to integrate OIM with OAM.

   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 Oracle Internet Directory.
     - `OUD` if your Identity Store is Oracle Unified Directory.
     - `ACTIVE_DIRECTORY` if your Identity Store is Microsoft Active Directory
   - **Directory Server ID**: A name for your directory server. For example: `IdStore`. This is only required if the directory type is `OID` or `OUD`
   - **Server URL**: The LDAP server URL. For example:

     ```
     ldap://idstore.example.com:1389 for OUD
     ldap://idstore.example.com:3060 for OID
     ```

   - **Server User**: The user name for connecting to the LDAP Server. This is the `OIMLDAPUSER` from the worksheet. For example:

     ```
     cn=oimLDAP,cn=systemids,dc=example,dc=com
     ```

   - **Server Password**: The password for connecting to the LDAP Server.
   - **Server Search DN**: The Search DN. This is the `REALM_DN` from the worksheet. For example:

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

Click **Next**.

> **Note:** Ensure that you have configured the directory according to the documentation and click **OK** on the pop up message displayed:
> `Ensure that you have a supported Directory server and that you have pre-configured the Directory as per the documentation and it is available for the installer.`

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. this is the *GROUPS_CONTAINER* from the worksheet. For example:

     `cn=Groups,dc=example,dc=com`

   - **LDAP User Container**: The DN for the User Container. This is the container where the Oracle Identity Manager users are stored. This is the *USERS_CONTAINER* from the worksheet. For example:

     `cn=Users,dc=example,dc=com`

   - **User Reservation Container**: The DN for the User Reservation Container. This is the *RESERVE_CONTAINER* from the worksheet. For example:

     `cn=Reserve,dc=example,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 Wizard.

19.3 Copying SOA Composites to Managed Server Directory

When SOA first starts, it automatically deploys a number of applications that are located in the *IGD_ASERVER_HOME*`/soa` directory. Performing `pack` and `unpack` does not populate this directory, so you must create it manually.

Copy the `soa` directory from *IGD_ASERVER_HOME*`/IAMGovernanceDomain/soa` to *IGD_MSERVER_HOME*`/IAMGovernanceDomain`.

For example:

```
cp -rp /u01/oracle/config/domains/IAMGovernanceDomain/soa
/u02/private/oracle/config/domains/IAMGovernanceDomain/soa
```

Perform these steps on all OIMHOSTs.

Restart the WLS_SOA1 and WLS_SOA2 servers.

19.4 Modifying the Oracle Identity Manager Properties to Support Active Directory

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*.

19.5 Starting and Validating Oracle Identity Manager on OIMHOST1

Start the Oracle Identity Manager Managed Server on OIMHOST1. This involves the following tasks:

1. Starting the Node Manager on OIMHOST1, if it is not already running.
2. Restarting the WebLogic Administration Server on OIMHOST1.
3. Restarting the SOA Managed Server wls_soa1 on OIMHOST1.
4. Starting the OIM Managed Server wls_oim1 on OIMHOST1.

For information about starting and stopping servers, see Section 31.1.6, "Starting and Stopping IAMGovernanceDomain Services".

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

```
http://OIMHOST1VHN1.example.com:14000/identity/
http://OIMHOST1VHN1.example.com:14000/sysadmin/
```

Log in using the `xelsysadm` username and password.

Validate the SOA configuration at

```
http://OIMHOST1VHN2.example.com:8001/soa-infra
```

Log in as the weblogic user.

19.6 Starting and Validating Oracle Identity Manager on OIMHOST2

Start the Oracle Identity Manager Managed Server on OIMHOST2. This involves the following tasks:

1. Starting the Node Manager on OIMHOST2, if it is not already running.
2. Restarting the SOA Managed Server wls_soa2 on OIMHOST2.
3. Starting the OIM Managed Server wls_oim2 on OIMHOST2.

For information about starting and stopping servers, see Section 31.1.6, "Starting and Stopping IAMGovernanceDomain Services".

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

```
http://OIMHOST2VHN1.example.com:14000/identity/
http://OIMHOST2VHN1.example.com:14000/sysadmin/
```

Log in using the xelsysadm username and password.

Validate the SOA configuration at

http://OIMHOST2VHN2.example.com:8001/soa-infra

Log in as the weblogic user.

19.7 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 *IGD_ORACLE_HOME*/server/ldap_config_util directory. Run the Script on OIMHOST1 as follows:

1. Edit the ldapconfig.props file located under the *IDG_ORACLE_HOME*/server/ldap_config_util directory and provide the following values:

Parameter	Value	Description
OIMProviderURL	t3://OIMHOST1VHN1.example.com:14000,OIMHOST2VHN1.example.com:14000	List of Oracle Identity Manager managed servers
LIBOVD_PATH_PARAM	*IGD_ASERVER_HOME*/config/fmwconfig/ovd/oim	Location of LIBOVD configuration files.

2. Save the file.
3. Set the JAVA_HOME, WL_HOME, MW_HOME, APP_SERVER, OIM_ORACLE_HOME, and DOMAIN_HOME environment variables, where:
   - JAVA_HOME is set to *IGD_MW_HOME*/jdk
   - WL_HOME is set to *IGD_MW_HOME*/wlserver_10.3
   - APP_SERVER is set to weblogic
   - OIM_ORACLE_HOME is set to *IGD_ORACLE_HOME*
   - DOMAIN_HOME is set to *IGD_ASERVER_HOME*
   - MW_HOME is set to *IGD_MW_HOME*
4. Run LDAPConfigPostSetup.sh. The script prompts for the Oracle Internet Directory admin password and the Oracle Identity Manager admin password. For example:

   IGD_ORACLE_HOME/server/ldap_config_util/LDAPConfigPostSetup.sh *path_to_property_file*

   For example:

   cd *IGD_ORACLE_HOME*/server/ldap_config_util/
   ./LDAPConfigPostSetup.sh *IGD_ORACLE_HOME*/server/ldap_config_util

   If the script is executed successfully, a success message similar to following is shown:

   "Successfully Enabled Changelog based Reconciliation schedule jobs.
   Successfully Updated Changelog based Reconciliation schedule jobs with last change number:"

5. Ignore the following errors:

```
java.lang.ClassNotFoundException:
oracle.as.jmx.framework.standardmbeans.spi.JMXFrameworkProviderImpl
```

19.8 Configuring 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:

```
RT_HOME/domains/IAMGovernanceDomain/tlogs/cluster_soa
RT_HOME/domains/IAMGovernanceDomain/tlogs/cluster_oim
```

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 appears.
5. Click the name of either the **Oracle Identity Manager** (wls_oimn) or the **SOA server** (wls_soan) represented as a hyperlink in the **Name** column of the table.

   The Settings page for the selected server appears.
6. Go to the **Configuration** tab.
7. Click **General** and then go to the **Services** 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:

   ```
   RT_HOME/domains/IAMGovernanceDomain/tlogs/cluster_oim
   ```

   For SOA Servers:

   ```
   RT_HOME/domains/IAMGovernanceDomain/tlogs/cluster_soa
   ```

> **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**.
10. Repeat the above steps to update Default store Directory for all OIM and SOA managed servers.
11. Activate the changes.

19.9 Configuring UMS Email

This section describes how to configure UMS email notification. This is optional. 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 the Oracle Enterprise Manager Fusion Middleware Control instance that is associated with Oracle Identity Manager.
2. Expand **User Messaging Service**.
3. Right click **usermessagingdriver-email (wls_soa1)** and select **email driver properties.**
4. Enter the following information:
   - **OutgoingMailServer**: name of the SMTP server, for example: smtp.example.com
   - **OutgoingMailServerPort**: port of the SMTP server, for example: 465 for SSL outgoing mail server and 25 for non-SSL
   - **OutgoingMailServerSecurity**: The security setting used by the SMTP server. Possible values can be None/TLS/SSL. If the mail server is configured to accept SSL requests, perfom these additional steps to remove DemoTrust store references from the SOA environment:

     Modify the *IGD_ASERVER_HOME*/domain_name/bin/setDomainEnv.sh file to remove the DemoTrust references:

     ```
     -Djavax.net.ssl.trustStore=IGD_WL_HOME/server/lib/DemoTrust.jks
     ```

     from EXTRA_JAVA_PROPERTIES.

     Restart both the Administration server and the Managed server.
   - **OutgoingUsername**: Any valid username
   - **OutgoingPassword**:

     Choose **Indirect Password**, **Create New User**.

     Provide a unique string for Indirect Username/Key, for example: OIMEmailConfig. This masks the password and not expose it in cleartext in the configuration file.

     Provide valid password for this account.

     Click **Apply**.

     Repeat Steps 3 and 4 for each SOA server.
5. From the Navigator, select **WebLogic Domain**, and then **DomainName**.
6. From the menu, select **System Mean Browser**.
7. Expand **Application Defined MBeans**, **oracle.iam**, **Server**, **wls_oim1**, **Application: oim**, and then **IAMAppRuntimeMBean**.
8. Click **UMSEmailNotificationProviderMBean**.

Enter the following:

- **Web service URL**: `http://igdinternal.example.com:80/ucs/messaging/webservice`
- **Policies**: Leave blank.
- **CSFKey**: `Notification.Provider.Key`

Click **Apply**.

19.10 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.

1. Log in to the WebLogic administration console.
2. Select **Clusters** from the home page or, alternatively, select **Environment** and then **Clusters**, from the **Domain Structure** menu.
3. Click **Lock & Edit** in the Change Center Window to enable editing.
4. Click the **Cluster Name** (cluster_soa).
5. In the **Configuration** tab, select the **HTTP** subtab and enter the following:

   Frontend Host: `igdinternal.example.com`

   Frontend HTTP Port: `7777`
6. Click **Save**.
7. Click **Activate Changes** in the Change Center window.

19.11 Restarting the Administration Server, Oracle Identity Manager, and Oracle SOA Suite Servers

Restart the WebLogic Administration Server, Oracle SOA Suite Managed Servers, and the Oracle Identity Manager Managed Servers on OIMHOST1 and OIMHOST2.

For information about starting and stopping servers, see Section 31.1.6, "Starting and Stopping IAMGovernanceDomain Services".

19.12 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://prov.example.com:443/identity`

and

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

Log in using the `xelsysadm` username and password.

19.13 Integrating Identity Manager with Access Manager

This section describes how to integrate Identity Manager with Access Manager.

This section contains the following topics:

19.13.1 Copying OAM Keystore Files to OIMHOST1 and OIMHOST2

If you are using Access Manager with the Simple Security Transport model, copy the OAM keystore files that were generated in Section 17.4, "Creating Access Manager Key Store.". Copy the keystore files *SHARED_CONFIG_DIR*`/keystores/ssoKeystore.jks` and *IAD_ASERVER_HOME*`/output/webgate-ssl/oamclient-truststore.jks` to the directory *IGD_MSERVER_HOME*`/config/fmwconfig` on OIMHOST1 and OIMHOST2.

19.13.2 Updating Existing LDAP Users with Required Object Classes

You must update existing LDAP users with the object classes OblixPersonPwdPolicy, OIMPersonPwdPolicy, and OblixOrgPerson.

Note: This step is not required in case of a fresh setup where you do not have any existing users.

To update the existing LDAP user, complete the following steps:

1. On OAMHOST1, create a properties file for the integration called `user.props`, with the following content:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 1389
IDSTORE_ADMIN_USER: cn=orcladmin
IDSTORE_DIRECTORYTYPE:OUD, OID
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
PASSWORD_EXPIRY_PERIOD: 7300
IDSTORE_LOGINATTRIBUTE: uid
```

   In this example:

   - `IDSTORE_HOST` is the name of LDAP server. For example: `idstore.example.com`
   - `IDSTORE_PORT` is the port of the LDAP server.
   - `IDSTORE_ADMIN_USER` is the bind DN of an administrative user. For example `cn=orcladmin` or `cn=oudadmin`
   - `IDSTORE_DIRECTORYTYPE` is the type of directory. The valid values are `OUD` and `OID`.
   - `IDSTORE_USERSEARCHBASE` is the location of users in the directory. For example `cn=Users,dc=example,dc=com`

- IDSTORE_GROUPSEARCHBASE is the location of groups in the directory. For example cn=Groups,dc=example,dc=com
- IDSTORE_LOGINATTRIBUTE this is the directory login attribute name. For example uid
- PASSWORD_EXPIRY_PERIOD is the password expiry period

2. Set the environment variables MW_HOME, JAVA_HOME, and ORACLE_HOME. For example:

   set ORACLE_HOME to *IAM_ORACLE_HOME*

3. Upgrade the existing LDAP by running the following command *IAM_ORACLE_HOME*/idmtools/bin:

   idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=*configfile*

   For example:

   idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=user.props

   When prompted, enter the password of the user you are using to connect to your Identity Store.

   Note: If the following error is displayed when running the command, ignore the error:

   ```
   java.lang.ClassNotFoundException:
   oracle.as.jmx.framework.standardmbeans.spi.JMXFrameworkProviderImpl
   at java.net.URLClassLoader$1.run(URLClassLoader.java:202)
   ```

19.13.3 Importing OIM certificates into Mobile Security Suite

Mobile Security Suite must be able to trust Oracle Identity Manager. In order to do this import the IAMGovernanceDomain certificate into MSAS. To do this, perform the following steps.

- Section 19.13.3.1, "Obtaining JPS Credential Store Password for IAMAccessDomain."
- Section 19.13.3.2, "Exporting IAMGovernanceDomain Certificate."
- Section 19.13.3.3, "Importing Certificate into IAMAccessDomain."

19.13.3.1 Obtaining JPS Credential Store Password for IAMAccessDomain

To obtain the JSP Credential Store Password for IAMAccessDomain:

1. Login to Enterprise Manager Fusion Middleware Control for the IAMAccessDomain using the WebLogic Administrators account at the following URL:

   http://iadadmin.example.com/em

2. Navigate to **Farm_IAMAccessDomain**, **WebLogic Domain**, and then **IAMAccessDomain**.
3. Right click and click System MBean Browser.
4. Click the **Search** button and enter JpsCredentialStore and click **Search**.
5. Click on the **Operations** tab.
6. Click on **getPortableCredential**.

7. Enter the following values:

   P1: `oracle.wsm.security`

   P2: `keystore-csf-key`

8. Click **Invoke**.

9. Make a note of the returned Password.

19.13.3.2 Exporting IAMGovernanceDomain Certificate

Export the `IAMGovernanceDomain` certificate using the following `keytool` command:

```
keytool  -keystore IGD_ASERVER_HOME/config/fmwconfig/default-keystore.jks
-storepass <<PASSWORD>>  -exportcert -alias xell -file SHARED_CONFIG_
DIR/keystores/xell.crt
```

Where password is the password you supplied when creating the `IAMGovernanceDomain`.

19.13.3.3 Importing Certificate into IAMAccessDomain

Import the certificate extracted above into the IAMAccessDomain using the following command:

```
keytool -keystore IAD_ASERVER_HOME/config/fmwconfig/default-keystore.jks
-storepass <<PASSWORD>> -importcert -alias xell -file SHARED_
CONFIG/keystores/xell.crt
```

Where password is the password you obtained from Enterprise Manager Fusion Middleware Control above.

19.13.4 Integrating Access Manager and Mobile Security Suite with Oracle Identity Manager 11*g*

Integrating Oracle Identity Manager with Access Manager using a WebGate 11*g* profile employs an Access Manager Trusted Authentication Protocol (TAP) scheme. This is different from WebGate 10*g* which used Network Assertion Protocol (NAP).

To integrate Access Manager with Oracle Identity Manager, perform the following steps on OIMHOST1:

1. Set the Environment Variables: MW_HOME, JAVA_HOME and ORACLE_HOME. For example:

   ```
   set ORACLE_HOME to IGD_ORACLE_HOME
   set MW_HOME to IGD_MW_HOME
   ```

2. Create a properties file for the integration called `oimitg.props`, this file will have many of the same values as the file in Creating Configuration File the file should contain the following.

   ```
   LOGINURI: /${app.context}/adfAuthentication
   LOGOUTURI: /oamsso/logout.html
   AUTOLOGINURI: None
   ACCESS_SERVER_HOST: OAMHOST1.example.com
   ACCESS_SERVER_PORT: 5575
   ACCESS_GATE_ID: Webgate_IDM
   COOKIE_DOMAIN: .example.com
   COOKIE_EXPIRY_INTERVAL: 120
   IDSTORE_LOGINATTRIBUTE: uid
   OAM_TRANSFER_MODE: simple
   ```

```
WEBGATE_TYPE: ohsWebgate11g
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 1389
IDSTORE_HOST: idstore.example.com
IDSTORE_DIRECTORYTYPE: OUD, OID or AD
IDSTORE_ADMIN_USER: cn=oamLDAP,cn=systemids,dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_WLSADMINUSER: weblogic_idm
MDS_DB_URL: jdbc:oracle:thin:@(DESCRIPTION =
(ADDRESS=(PROTOCOL=TCP)(HOST=IGDDBSCAN.example.com)(PORT=1521)) (CONNECT_
DATA=(SERVICE_NAME=oimedg.example.com)))
MDS_DB_SCHEMA_USERNAME: edgigd_mds
WLSHOST: igdadminvhn.example.com
WLSPORT: 7101
WLSADMIN: weblogic
WLSPASSWD: password
OAM11G_WLS_ADMIN_HOST: IADADMINVHN.example.com
OAM11G_WLS_ADMIN_PORT: 7001
OAM11G_WLS_ADMIN_USER: weblogic
DOMAIN_NAME: IAMGovernanceDomain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: IGD_ASERVER_HOME
OIM_MSM_REST_SERVER_URL: http://iadinternal.example.com:7777/
```

Property Descriptions:

- `LOGINURI`: This is required by Oracle Platform Security Services (OPSS) and should always be set to `/${app.context}/adfAuthentication`
- `LOGOUTURI`: This is required by Oracle Platform Security Services (OPSS) and should always be set to `/oamsso/logout.html`
- `AUTOLOGINURI`: This is required by Oracle Platform Security Services (OPSS) and should always be set to `None`
- `ACCESS_SERVER_HOST`: This is the name of one of the Access Server hosts. If you have placed a load balancer in front of Oracle Access Manager Managed Servers, then specify the load balancer name for this property here. For example, `OAMHOST1.example.com`
- `ACCESS_SERVER_PORT`: This is the OAM Proxy Port (OAM_PROXY_PORT). For example, `5575`
- `ACCESS_GATE_ID`: This is the name of the Agent that gets created in Oracle Access Manager. This can be any value. For example, `Webgate_IDM`
- `COOKIE_DOMAIN`: This is the Oracle Access Manager cookie domain and should be proceeded by a period (`.`). For example, `.example.com`
- `COOKIE_EXPIRY_INTERNAL`: This is the number of seconds before a cookie expires and the user is forced to re-login. The default value is `120`. If you wish the cookie to never expire, set this value to `-1`.
- `IDSTORE_LOGINATTRIBUTE`: This is the LDAP attribute which is used to validate login. This is typically the `uid`.
- `OAM_TRANSFER_MODE`: This is the security mode that Oracle Access Manager is configured to work with. This is usually `Simple`. It should be the same value you placed into the Oracle Access Manager property file.
- `WEBGATE_TYPE`: This is the type of WebGate agent you wish to create. Valid values are `ohsWebgate10g` or `ohsWebgate11g`.

For Oracle Identity and Access Management 11.1.2.3.0, this is usually `ohsWebgate11g`. Note that, if you are using Oracle Traffic Director instead of Oracle HTTP Server, then it should still be `ohsWebgate11g`.

- `SSO_ENABLED_FLAG`: This value should be set to `true`.
- `IDSTORE_PORT`: This is the port on your load balancer where you are accepting LDAP requests. For example, `3060` or `1389`
- `IDSTORE_HOST`: This is the load balancer name fronting your LDAP directory
- `IDSTORE_DIRECTORYTYPE`: Set this property to `OID` if your Identity Store is in Oracle Internet Directory, `OUD` if you are connecting to Oracle Unified Directory, or `AD` if your identity Store is in Active Directory.
- `IDSTORE_ADMIN_USER`: This is the admin user of the ID store.
- `IDSTORE_USERSEARCHBASE`: This is the location in the directory where Users are Stored.
- `IDSTORE_GROUPSEARCHBASE`: This is the location in the directory where Groups are Stored.
- `IDSTORE_WLSADMINUSER`: This is the value you used when you prepared the identity store. For example `weblogic_idm`.
- `MDS_DB_URL`: Set this to the OIM database jdbc connection details. For example:

  ```
  jdbc:oracle:thin:@(DESCRIPTION =
  (ADDRESS=(PROTOCOL=TCP)(HOST=IGDDBSCAN.example.com)(PORT=1521))
  (CONNECT_DATA=(SERVICE_NAME=oimedg.example.com)))
  ```

- `MDS_DB_SCHEMA_USERNAME`: This is the username of the MDS schema.
- `WLS_HOST`: This is the Admin Server listen address. For OAM configuration this will be the host associated with the IAMAccessDomain. For OAM/OIM integration this will be the host associated with the IAMGovernanceDomain.
- `WLS_PORT`: This is the Admin Server listen port. For OAM configuration this will be the port associated with the IAMAccessDomain. For OAM/OIM integration this will be the host associated with the IAMGovernanceDomain.
- `WLS_ADMIN`: This is the user used to connect to the Admin Server
- `WLSPASSWD`: This is the password of the `WLS_ADMIN` account.
- `OAM11G_WLS_ADMIN_HOST`: This is the IAMAccessDomain Admin Server listen address.
- `OAM11G_WLS_ADMIN_PORT`: This is the IAMAccessDomain Admin Server listen port.
- `OAM11G_WLS_ADMIN_USER`: This is the IAMAccessDomain Administration User
- `DOMAIN_NAME`: This is the domain name. For example, `IAMGovernanceDomain`
- `OIM_MANAGED_SERVER_NAME`: This is the name of the Oracle Identity Manager Managed Server. For example, `wls_oim1`
- `DOMAIN_LOCATION`: This is the domain location. For example, *`IGD_ASERVER_HOME`*
- `OIM_MSM_REST_SERVER_URL`: This is the URL that the MSAS proxy server uses to invoke the MSM rest services. This is the entry point for Identity Access Domain callbacks. For example, `iadinternal.example.com:7777`

- SPLIT_DOMAIN: This is used when OAM and OIM are in different domains. This should always be set to true.

3. Integrate Access Manager with Oracle Identity Manager by running the following command from the location *IGD_ORACLE_HOME*/idmtools/bin:

   ```
   idmConfigTool.sh -configOIM input_file=configfile
   ```

   For example:

   ```
   idmConfigTool.sh -configOIM input_file=oimitg.props
   ```

   When prompted, enter the following information:

   - Password of the admin user of the IAMAccessDomain
   - SSO Access Gate Password
   - SSO Keystore Password
   - Global Passphrase
   - Idstore Admin Password
   - MDS Database schema password
   - OAM 11g Domain User Password

     This is the password of the weblogic_idm user.

4. Restart the IAMGovernanceDomain Administration Server, and the Managed Servers - WLS_SOA1, WLS_SOA2, WLS_OIM1, and WLS_OIM2.

19.13.5 Creating OMSS Helpdesk User and Roles

Once you have integrated OAM and OIM, create a user for Oracle Mobile Security Suite.

To create a user:

1. Log in to the OIM Self Service Console as the user xelsysadm, using the following URL:

   ```
   https://prov.example.com/identity
   ```

2. Click the **Manage** button on the top of the screen.
3. Click **Users** from the Launch Pad, and click **Create**.
4. Complete the information on the screen to create a user to be used for the OMSS helpdesk, and click **Submit**.
5. Go to the **Home** tab.
6. From the Launch Pad click **Administration Roles**, and click **Create**.
7. Enter the following Information into the Basic Information Screen:

   - **Name**: helpdesk
   - **Display Name**: helpdesk

   Click **Next**.
8. On the Capabilities screen, click **Add Capabilities**.
9. Enter **User - View** in the **Display Name** field and click **Search**.
10. Select **User - View / Search** from the search results and click **Add Selected**.

11. Repeat steps 10 and 11 to add the capability **Role - View / Search**
12. Click **Select**, and then click **Next**.
13. On the Members screen, click **Assign Users**.
14. Enter the name of your helpdesk user in the Search box and click **Search**.
15. Select the **helpdesk** user from the search results, click **Add Selected**, click **Select**, and then click **Next**.
16. On the Scope of Control screen click **Add Organizations**.
17. Enter an Organization in the Search box and click **Search**.
18. Select the required organization, click **Add Selected**, click **Select**, and then click **Next**.
19. On the Organizations screen click **Next**.
20. On the Summary screen click **Finish**.

19.13.6 Managing the Password of the xelsysadm User

After you integrate Oracle Identity Manager with Access Manager, two xelsysadm accounts exist. One is the internal account created by Oracle Identity Manager. The other is the account you created in the Identity Store.

The xelsysadm account located in the LDAP store is the one used to access the OIM console. If you want to change the password of this account, change it in LDAP. You can use Oracle Directory Service Manager (ODSM) to do this. Do not change it through the OIM console.

19.13.7 Validating Integration

To validate integration, you must assign Identity Management administrators to WebLogic security groups and install WebGate as described in Chapter 22, "Configuring Single Sign-On".

To validate that the wiring of Access Manager with Oracle Identity Manager 11*g* was successful, attempt to log in to the Oracle Identity Manager Self Service Console by doing the following:

1. Using a browser, navigate to the following URL:

   `https://prov.example.com/identity`

   This redirects you to the Oracle Access Manager 11*g* single sign-on page.
2. Log in using the xelsysadm user account created in Chapter 13, "Preparing The Identity Store".
3. If you see the OIM Self Service Console Page, the integration was successful.

19.14 Enabling OIM to Connect to SOA Using LDAP User

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 post installation 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:

> **Note:** For the SOAConfig Mbean to be visible, at least one OIM Managed Server must be running.

1. Log in to Enterprise Manager Fusion Middleware Control of the IAMGovernanceDomain, as the `weblogic` user
2. Select **Farm_IAMGovernanceDomain**, **WebLogic Domain**, and then **IAMGovernanceDomain**.
3. Right-click and **Select System MBean Browser** from the menu or right-click to select it.
4. Select **Search**, enter `SOAConfig`, then click **Search**.
5. Change the username attribute to the Oracle WebLogic Server administrator username provisioned in Preparing the Identity Store. For example:

   ```
   weblogic_idm
   ```

   Click **Apply**.
6. Select **Weblogic Domain**, and then **IAMGovernanceDomain**.
7. Select **Security** and then **Credentials** from the down menu.
8. Expand the key **oim**.
9. Click **SOAAdminPassword** and click **Edit**.
10. Change the username to `weblogic_idm` and set the password to the accounts password and click **OK**.
11. From the navigator, click **Farm_IAMGovernanceDomain** and then click **WebLogic Domain**. Right-click on **IAMGovernanceDomain**, and select **Application Roles** from the Security menu.
12. Set the application stripe to `soa-infra` by selecting from the drop-down list. Click **Search**.
13. Click **SOAAdmin**. Ensure that you see **Administrators** in the membership box.
14. Click **Edit**. The Edit page is displayed.
15. Click **Add** in the Members box. The Add principal search box is displayed.

    Enter the following:

    - Type: Group
    - Principal Name: starts with: IDM

    Click Search.
16. Select **IDM Administrators** from the results box and click **OK**.

    You will be redirected to the Edit screen. Ensure that the members are Administrators and IDM Administrators.

    Click **Ok**.
17. Run the reconciliation process to enable the Oracle WebLogic Server administrator, `weblogic_idm`, to be visible in the OIM Identity Console. Follow these steps:

a. Log in to the OIM System Administration Console as the user `xelsysadm`.

b. Click **Scheduler** under **System Configuration**.

c. Enter `LDAP*` in the search box.

d. Click the arrow for the **Search Scheduled Jobs** to list all the schedulers.

e. Select **LDAP User Create** and **Update Full Reconciliation**.

f. Click **Run Now** to run the job.

g. Repeat for the job **LDAP Role Create** and **Update Full Reconciliation**.

h. Log in to the OIM Identity Console and verify that the user **weblogic_idm** is visible.

18. Log in to the OIM Self service Console as the user `xelsysadm`.

    If prompted, set up challenge questions. This happens on your first login to Oracle Identity Manager Identity Console.

19. Click on **Roles** tab under **Manage** tab.

20. Search for the Administrators role.

    Enter `Administrators` into the **Display Name** search box and click **Search**.

21. Click the **Administrators Role**.

    That Role's Properties page appears.

22. Click on **Organizations** tab

23. Click **Add**. Search and select the organization to which `xelsysadm` belongs, example, **Xellerate Users**

24. Click **Add Selected**. Click **Select**.

25. Click the **Members** tab and click **Add**.

26. Search for the user `weblogic_idm` . Select the **weblogic_idm** user

27. Click **Add Selected**.

28. Click **Select**, and then **Apply**.

19.15 Updating OIM LDAP Reconciliation Jobs

To update the PIM LDAP reconciliation jobs, complete the following steps:

1. Open a browser and go to the following location:

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

2. Log in a as `xelsysadm` using the *`COMMON_IDM_PASSWORD`*.

3. Under **System Management**, click **Scheduler**.

4. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.

5. For each job in the search results, click on the job name on the left, then click **Disable** on the right.

   Do this for all jobs. If the job is already disabled do nothing.

6. Run the following commands on LDAPHOST1:

   `cd` *`LDAP_ORACLE_INSTANCE`*`/OUD/bin`

```
./ldapsearch -h ldaphost1 -p 1389 -D "cn=oudadmin" -b "" -s base
"objectclass=*" lastExternalChangelogCookie

Password for user 'cn=oudadmin': <OudAdminPwd>
dn: lastExternalChangelogCookie:
dc=example,dc=com:00000140c682473c263600000862;
```

Copy the output string that follows `lastExternalChangelogCookie:`. This value is required in the next step. For example,

```
dc=example,dc=com:00000140c682473c263600000862;
```

The Hex portion must be 28 characters long. If this value has more than one Hex portion then separate the 28char portions with spaces. For example:

```
dc=example,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
```

7. Run each of the following LDAP reconciliation jobs once to reset the last change number.:
   - LDAP Role Delete Reconciliation
   - LDAP User Delete Reconciliation
   - LDAP Role Create and Update Reconciliation
   - LDAP User Create and Update Reconciliation
   - LDAP Role Hierarchy Reconciliation
   - LDAP Role Membership Reconciliation

   To run the jobs:

   a. Login to the OIM System Administration Console as the user `xelsysadm`.
   b. Under **System Configuration**, click **Scheduler**.
   c. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
   d. Click on the job to be run.
   e. Set the parameter **Last Change Number** to the value obtained in step 6.

      For example:

      ```
      dc=example,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
      00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
      ```

   f. Click **Run Now**.
   g. Repeat for each of the jobs in the list at the beginning of this step.
8. For each incremental recon job whose last changelog number has been reset, execute the job and check that the job now completes successfully.
9. After the job runs successfully, re-enable periodic running of the jobs according to your requirements.

19.16 Updating the Username Generation Policy for Active Directory

If your back end directory is Active Directory, you must update Oracle Identity Manager so that it only allows user names with a maximum of 20 characters. This is a

limitation of Active Directory. Update the username generation policy from DefaultComboPolicy to FirstnameLastnamepolicyforAD by doing the following:

1. Log in to the OIM Administration Console.
2. Go to **System Configuration** tab, and click **Configuration Properties**.
3. In the **Search** box, enter **Default Policy for Username Generation** and click **Search**.
4. Click **Default Policy for Username Generation**.
5. In the **Value** field, update the entry:

   from

   `oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy`

   to

   `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD`
6. Click **Save**.

19.17 Excluding Users from Oracle Identity Manager Reconciliation

By default Oracle Identity Management reconciles all users that are located in the LDAP container cn=Users. Once reconciled, these users are subject to the usual password ageing policies defined in Oracle Identity Manager. This is not desirable for system accounts. It is recommended that you exclude the following accounts from this reconciliation:

- xelsysadm
- oimLDAP
- oamLDAP

Additionally, you might want to exclude:

- IDRUser
- IDRWUser
- PolicyROUser
- PolicyRWUser

To exclude these users from reconciliation and discard failed reconciliation events, add `orclAppIDUser` object class to each of the above users, so that they are excluded from reconciliation.

Closing Failed Reconciliation Events by Using the OIM Console

1. Log in to the OIM Administration Console as the `xelsysadm` user.
2. Click **Reconciliation** under **Provisioning Configuration**.
3. Click **Advanced Search**.
4. In the **Current Status** field, select **Equals**. In the **Search** box, select **Creation Failed** from the list, and click **Search**.
5. Select each of the events.
6. From the **Actions** menu, select **Close Event**.

7. In the **Confirmation** window enter a justification, such as **Close Failed Reconciliation Events** and click **Closed**.
8. Click **OK** to acknowledge the confirmation message.

19.18 Closing Failed Reconciliation Events Using OIM Console

Complete the following steps to close the failed reconciliation events:

1. Log in to the OIM Administration Console as the xelsysadm user.
2. Click **Reconciliation** under **Provisioning Configuration**.
3. Click **Advanced Search**.
4. In the **Current Status** field, select **Equals**. In the **Search** box, select **Creation Failed** from the list.
5. Click **Search**.
6. For each of the events, select **Close Event** from the **Actions** menu.
7. In the **Confirmation** window, enter a justification. For example, `Close Failed Reconciliation Events`.
8. Click **Closed**.
9. Click **OK** to acknowledge the confirmation message.

19.19 Using JDBC Persistent Stores for TLOGs and JMS

For information about when to use JDBC persistent stores for transaction logs (TLOGs) and JMS, and for instructions on how to configure the persistent stores for TLOGS and JMS for Oracle Identity Manager Managed Servers, see Section 15.4.10, "Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment".

19.20 Enabling Exalogic Optimizations

This section describes post-deployment steps for Exalogic implementations.

This section includes the following topics:

- Configuring Oracle Identity Manager Servers to Listen on EoIB
- Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager and SOA

19.20.1 Configuring Oracle Identity Manager Servers to Listen on EoIB

This section is only required if the Oracle Identity Manager servers need to be accessed directly from outside the Exalogic machine. This is the case when external Oracle HTTP Servers are part of the configuration.

Create a new network channel as follows:

1. Log in to the WebLogic Console in the IAMGovernanceDomain.
2. Click **Lock & Edit**.
3. Navigate to **Environment -> Servers** to open the Summary of Servers page
4. In the Servers table, click **WLS_OIM1**.
5. Select **Protocols** and then **Channels**.

6. Click **New** to create a new channel.
7. Enter `OIMHOST1VHN-EXTCHAN` as the name. Select **HTTP** as the protocol and click **Next**.
8. In the Network Channel Addressing page, enter the following information:
   - **Listen Address**: `OIMHOST1VHN-EXT`

     This is the bond1 address assigned to OIMHOST1VHN-EXT
   - **Listen Port**: `8001`
9. Click **Next** and select the following in the Network Channel Properties page:
   - Enabled
   - HTTP Enabled for this protocol
10. Click **Finish**.
11. Click **Activate Changes**.

Repeat the preceding steps, substituting **WLS_OIM2** and `OIMHOST2VHN-EXT` for the Server and Listen Address.

19.20.2 Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager and SOA

You can enable session replication enhancements for Managed Servers in a WebLogic cluster to which you deploy a Web application at a later time.

To enable session replication enhancements for `oim_cluster` in the domain IAMGovernanceDomain, use the values in Table 19–2.

Table 19–2 Network Channel Properties

Managed Server	Name	Protocol	Listen Address	Listen Port	Additional Channel Ports
WLS_OIM1	`Replication Channel`	t3	OIMHOST1VHN1.example.com	7005	7006 to 7014
WLS_OIM2	`Replication Channel`	t3	OIMHOST2VHN1.example.com	7005	7006 to 7014
WLS_SOA1	`Replication Channel`	t3	OIMHOST1VHN2.example.com	7005	7006 to 7014
WLS_SOA2	`Replication Channel`	t3	OIMHOST2VHN2.example.com	7005	7006 to 7014

Proceed as follows:

1. Log in to the WebLogic Administration console at: `http://IGDADMIN.example.com/console`
2. Ensure that Managed Servers in the `oim_cluster` cluster are up and running, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
3. To set replication ports for a Managed Server, use the values in Table 19–2.

   To set the values for `WLS_OIM1`, for example, complete the following steps:

a. Under **Domain Structure**, click **Environment** and **Servers**. The Summary of Servers page is displayed.

b. Click **Lock & Edit**.

c. Click `WLS_OIM1` on the list of servers. The Settings for WLS_OIM1 are displayed.

d. Click the **Cluster** tab.

e. In the **Replication Ports** field, enter a range of ports for configuring multiple replication channels. For example, replication channels for Managed Servers in `oim_cluster` can listen on ports starting from `7005` to `7015`. To specify this range of ports, enter `7005-7015`.

f. Repeat Steps **a** through **e** for each of the other managed servers in Table 19–2.

4. The following steps show how to create a network channel for the managed server WLS_OIM1.

a. Log in to the Oracle WebLogic Server Administration Console.

b. If you have not already done so, click **Lock & Edit** in the Change Center.

c. In the left pane of the Console, expand **Environment** and select **Servers**.

The **Summary of Servers page** is displayed.

d. In the Servers table, click **WLS_OIM1** Managed Server instance.

e. Select **Protocols**, and then **Channels**.

f. Click **New**.

g. Enter **ReplicationChannel** as the name of the new network channel and select **t3** as the protocol, then click **Next**.

h. Enter the following information:

Listen address: **OIMHOST1VHN1**

Note: This is the WLS_OIM1 floating IP assigned to WebLogic Server.

Listen port: **7005**

i. Click **Next**, and in the Network Channel Properties page, select **Enabled** and **Outbound Enabled**.

j. Click **Finish**.

k. Click **Save**.

l. Under the **Network Channels** table, select **ReplicationChannel**, the network channel you created for the WLS_OIM1 Managed Server.

Expand **Advanced**, select **Enable SDP Protocol**, and click **Save**.

m. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

You must repeat the above steps to create a network channel each for the remaining Managed Servers in the cluster. Enter the required properties, as described in Table 19–2.

5. After creating the network channel for each of the Managed Servers in your cluster, click **Environment** > **Clusters**. The Summary of Clusters page is displayed.
6. Click oim_cluster. The Settings for oim_cluster page is displayed.
7. Click the **Replication** tab.
8. In the **Replication Channel** field, ensure that `ReplicationChannel` is set as the name of the channel to be used for replication traffic.
9. In the **Advanced** section, select the **Enable One Way RMI for Replication** option.
10. Click **Save**.
11. Repeat these steps for the SOA cluster and BI cluster.
12. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
13. Manually add the system property `-Djava.net.preferIPv4Stack=true` to the **startWebLogic.sh** script, which is located in the `bin` directory of *`IGD_ASERVER_HOME`*, using a text editor as follows:
    a. Locate the following line in the `startWebLogic.sh` script:

    ```
    . ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
    ```

    b. Add the following property immediately after the above entry:

    ```
    JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.net.preferIPv4Stack=true"
    ```

    c. Save the file and close.
14. Restart the Administration Server of the IAMGovernanceDomain and the Managed Servers - WLS_OIM1, WLS_OIM2, WLS_SOA1, WLS_SOA2.

19.21 Forcing OIM to use Correct Multicast Address

Oracle Identity Manager uses multicast for certain functions. By default, the managed servers communicate using the multi cast address assigned to the primary host name. If you wish multicast to use a different network, for example, of the internal network, you must complete the following additional steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://`*`IGDADMIN.example.com`*`/console`
2. Under **Domain Structure**, click **Environment** and then expand **Servers**. The Summary of Servers page is displayed.
3. Click **Lock & Edit**.
4. Click the OIM Managed Server name, for example, `WLS_OIM1` on the list of servers. The Settings for WLS_OIM1 are displayed.
5. Go to the **Server Start** tab.
6. Add the following line to the arguments field:

   ```
   -Dmulticast.bind.address=oimhost1vhn1
   ```
7. Click **Save**.
8. Repeat for the Managed Server `WLS_OIM2`. When doing so, make sure you add the following line to the arguments field:

   ```
   -Dmulticast.bind.address=oimhost2vhn1
   ```

9. Click **Activate Changes** and restart the managed servers `WLS_OIM1` and `WLS_OIM2`.

19.22 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 information on database backups, refer to your database documentation.

To back up the installation to this point, back up the following:

- The Web tier
- The Access Manager database.
- The Administration Server domain directory
- The Managed Server domain directory
- The LDAP Directory
- The Keystores created

20

Configuring BI Publisher

This chapter describes how to configure Oracle BI Publisher.

In Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0), Oracle Identity Manager comes with a bundled version of Business Intelligence to allow the production of governance reports. The bundled version is a subset of the Business Intelligence product.

BI Publisher is deployed and configured as a separate managed server within the same Oracle Identity Manager domain. You have the choice of either leveraging the embedded BI Publisher or a standalone BI Publisher. It is recommended that you use the embedded BI Publisher if there are no other reporting requirements, and you only need reporting for Oracle Identity Manager.

After you configure BI Publisher, you can use the following standard features of BI Publisher:

- Highly formatted and professional quality reports with pagination and headers/footers.
- PDF, Word, and HTML output of reports.
- Capability to develop your own custom reports against the Oracle Identity Manager repository (read-only repository access).
- BI Publisher's scheduling capabilities and delivery mechanisms, such as e-mail and FTP.
- Format (report) can be edited separately from the data definition (data model).
- Standardized Oracle Identity sub-template for headers.
- National Language Support (NLS) for BI Publisher report output.

This chapter describes how to configure BI Publisher to facilitate the creation of Identity Governance reports.

The Oracle Business Intelligence (BI) configuration is located in the Domain configuration directory. Perform the steps below to configure BI managed servers to use the BI configuration located under the *IGD_ASERVER_HOME*.

The WebLogic Administration Server automatically copies configuration changes applied to the primary domain configuration location to all the managed server domain configuration directories that have been registered to be part of the domain.

About Domain URLs

Table 20–1 lists the Domain URLs and their corresponding components and SSO Users.

Table 20–1 Domain URL Details

Component	URL	SSO User
Self-service Console	`https://prov.example.com/identity`	xelsysadm
OIM Administration Console	`http://igdadmin.example.com/sysadmin`	xelsysadm

20.1 Moving Reports to a Shared Directory

The BI Publisher configuration folder stores the files that contain your server configuration settings, for example, your data source connections, delivery server definitions, and scheduler settings.

The path to the configuration folder is stored in the `xmlp-server-config.xml` configuration file. When you install BI Publisher, this is automatically configured to:

`${xdo.server.config.dir}/repository`

The environment variable `${xdo.server.config.dir}` is used to store the path to the location of the `xmlp-server-config.xml` configuration file. By default, both the BI Publisher configuration folder and the `xmlp-server-config.xml` file are installed to *`DOMAIN_HOME`*`/config/bipublisher`. The resource section in the `xmlp-server-config.xml` defines the location of your repository.

By Default, the reports repository path in `xmlp-server-config.xml` is set to file system absolute path *`IGD_ASERVER_HOME`*`/config/bipublisher/repository`.

By default, Oracle BI Publisher stores reports on the local file system. In an highly available solution, this directory should be moved to a shared storage, so that all BI Publisher instances have access to the same report repository.

To set the server configuration options for Oracle BI Publisher, complete the following steps:

1. Shutdown BI managed servers `wls_bi1` and `wls_bi2` through the WebLogic Administration Console.
2. Edit the file `xmlp-server-config.xml`.

   `IGD_ASERVER_HOME``/config/bipublisher/xmlp-server-config.xml`

   Update the parameter 'path' in `xmlp-server-config.xml` file to reflect the shared configuration folder location.

```
 <?xml version = '1.0' encoding = 'UTF-8'?>
<xmlpConfig xmlns="http://xmlns.oracle.com/oxp/xmlp">
   <resource>
      <file path="IGD_ASERVER_HOME/config/bipublisher/repository"/>
   </resource>
```

```
   <config>
      <file path="IGD_ASERVER_HOME/config/bipublisher/repository"/>
   </config>
</xmlpConfig>
```

3. Save the `xmlp-server-config.xml` file.

> **Note:** Since the repository is in the file system, the case sensitivity of folder and report names is determined by the platform on which you run BI Publisher. For UNIX-based environments, the repository object names are case-sensitive.

20.1.1 Starting BI Publisher Managed Servers

Start the BI Publisher Managed Servers `wls_bi1` and `wls_bi2` on both OIMHOST1 and OIMHOST2.

For more information about starting the servers, see Section 31.1.6.4.1, "Starting Oracle BI Publisher WebLogic Managed Servers".

20.1.2 Validating the BI Server

Validate BI Publisher at the following URLs:

```
http://OIMHOST1VHN3.example.com:9704/xmlpserver
http://OIMHOST2VHN3.example.com:9704/xmlpserver
```

Log in as the `xelsysadm` user.

20.1.3 Validating BI Server Configuration

To validate the BI server configuration:

1. On OIMHOST1 log in to BI Publisher with `xelsysadm` credentials and select the **Administration** tab.
2. Under **System Maintenance**, select **Server Configuration**.
3. In the **Path** field under **Configuration Folder**, verify the shared location for the Configuration Folder. It must be the location provided in the `xmlp-server-config.xml` file.
4. In the **BI Publisher Repository** field under **Catalog**, verify the shared location for the BI Publisher Repository. It must be the location provided in the `xmlp-server-config.xml` file.
5. Repeat steps 1-4 on OIMHOST2.

20.2 Configuring BI Scheduler

The architecture of the BI Publisher Scheduler uses JMS queues and topics to provide a highly scalable, highly performing, and robust report scheduling and delivery system. BI uses the Quartz scheduling engine for scheduling the reports.

BI Publisher clustering support enables you to add server instances on demand to handle processing and delivery load. In a clustered implementation, the report repository and the scheduler database are shared across the multiple instances. Also, the JMS queues for scheduling and JMS topic for publishing diagnostic information are shared across the server by registering JMS queues and topics via JNDI services.

This section describes how to configure the scheduler options and JMS configuration.

This section contains the following topics:

- Section 20.2.1, "Setting Scheduler Configuration Options"
- Section 20.2.2, "Configuring JMS for BI Publisher"
- Section 20.2.3, "Configuring Default Persistence Store for Transaction Recovery"
- Section 20.2.4, "Using JDBC Persistent Stores for TLOGs and JMS"
- Section 20.2.5, "Updating the JMS Configuration of BIP Scheduler"

20.2.1 Setting Scheduler Configuration Options

Follow the below steps to configure the scheduler options:

1. On OIMHOST1, access the BI Publisher URL and log in as `xelsysadmin`.

   ```
   http://OIMHOST1VHN3.example.com:9704/xmlpserver
   ```

2. Select the **Administration** tab.
3. Under **System Maintenance**, select **Scheduler Configuration**.
4. Select **Quartz Clustering** under the **Scheduler Selection**, then click **Apply**.
5. Repeat these steps on OIMHOST2.

20.2.2 Configuring JMS for BI Publisher

Because of a known issue, when BI is configured only one persistence store is created. The workaround is to create a new persistent store using the following steps.In this procedure; you create a JMS store for BI for each managed server. One JMS store configuration is already created during WebLogic domain creation. The location for all persistence stores should be set to a directory that is visible from all BI nodes.

1. Shutdown all the BI Publisher Managed Servers. For more information, see Section 31.1.6.4.2, "Stopping Oracle BI Publisher WebLogic Managed Servers".
2. Create the following directory:

   ```
   RT_HOME/domains/IAMGovernanceDomain/jms/BipJmsStore1
   ```

3. Log into the WebLogic Administration Console.
4. In the Domain Structure window, expand the **Services** node and click the **Persistent Stores** node.
5. Click **Lock & Edit** in the **Change Center**.
6. In the Domain Structure window, expand the **Services** node and click the **Persistent Stores** node.
7. Click on existing File Store (for example, **BipJmsStore**), and verify the target. If it is WLS_BI2, the new File Store must target WLS_BI1.
8. Click **New** and **Create File Store**.
9. Enter a name, such as `BipJmsStore1` and target WLS_BI1. Note that the targets WLS_BI1 and WLS_BI1 (migratable) are displayed. Select WLS_BI1

   Enter a directory located in shared storage so that OIMHOST1 and OIMHOST2 can access it. For example:

   ```
   RT_HOME/domains/IAMGovernanceDomain/jms/BipJmsStore1
   ```

Click **Save**.

10. In the Domain Structure window, expand the **Services** node, expand **Messaging** and click **JMS Servers**.
11. Click **New**.

    Enter a name, such as `BipJmsServer1`.

    In the **Persistence Store** drop-down list, select **BipJmsStore1** and click **Next**.

    Select **WLS_BI1** as the target and click **Finish**.
12. In the Domain Structure window, expand the **Services** node, expand **Messaging** and click **JMS Modules** node.

    Click **BipJmsResource** and click the **Subdeployments** tab.

    Click **BipJmsSubDeployment** under the **Name** section of the subdeployments table.

    On the **Settings for BipJmsSubDeployment** page, under **JMS Servers** category, select the new JMS server that you created in the earlier steps. For example: BipJmsServer1.
13. Click **Save**, and then click **Activate Changes**.
14. Start the BI Publisher Managed Servers - wls_bi1 and wls_bi2. For information about starting the BI Publisher Managed Servers, see Section 31.1.6.4.1, "Starting Oracle BI Publisher WebLogic Managed Servers".

20.2.3 Configuring Default Persistence Store for Transaction Recovery

The WLS_BI 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. Preferably, this location should be on a dual-ported SCSI disk or on a Storage Area Network (SAN).

Perform the following steps to set the location for the default persistence stores for the BI Servers:

1. Create the following directory on the shared storage:

   RT_HOME`/domains/IAMGovernanceDomain/tlogs/cluster_bi`
2. Log in to the Oracle WebLogic Server Administration Console.
3. Click **Lock and Edit**.
4. Under **Domain Structure**, expand **Environment**, and then click **Servers**.

   The Summary of Servers page appears.
5. Click the name of the BI server (`wls_bin`) represented as a hyperlink in the **Name** column of the table.

   The Settings page for the selected server appears, and defaults to the Configuration tab.
6. Go to the **Services** sub tab.

7. 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:

   RT_HOME/domains/IAMGovernanceDomain/tlogs/cluster_bi

   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.

8. Click **Save**.

20.2.4 Using JDBC Persistent Stores for TLOGs and JMS

For information about when to use JDBC persistent stores for transaction logs (TLOGs) and JMS, and for instructions on how to configure the persistent stores for TLOGs and JMS for the BI Managed Servers, see Section 15.4.10, "Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment".

20.2.5 Updating the JMS Configuration of BIP Scheduler

The architecture of the BI Publisher Scheduler uses JMS queues and topics to provide a highly scalable, highly performing, and robust report scheduling and delivery system. BI Publisher clustering support enables you to add server instances on demand to handle processing and delivery load. The JMS queues for scheduling and JMS topic for publishing diagnostic information are shared across the server by registering JMS queues and topics through JNDI services. A shared Directory is used to temporarily store data and files used by the scheduler while jobs are executing. After a job is completed, the temporary data for the job is deleted. The directory is used to exchange data and document information among all the BI Publisher nodes and therefore, must be accessible by all BI Publisher nodes. The size of the directory depends on the total size of the job data, output documents, and the number of concurrent jobs. The directory should be big enough to hold all the XML data and documents for all the parallel running jobs. If BI Publisher runs on different machines while this directory is not configured, the scheduler may fail.

If BI Publisher runs on a single machine, defining a shared directory is optional. BI Publisher uses the application server's temporary directory to store this data.

Complete the following steps to configure the BI scheduler JMS configuration. Run this procedure on both OIMHOSTs: OIMHOST1 and OIMHOST2.

1. Log in to BI Publisher at the one of the following URLs:

   ```
   http://OIMHOST1VHN3:9704/xmlpserver
   http://OIMHOST2VHN3:9704/xmlpserver
   ```

2. Click **Administration** in the top right corner, then click **Scheduler Configuration** under **System Maintenance** to open the Scheduler Configuration page.

3. In the JMS Configuration section, update the Shared Directory by entering a directory that is located in the shared storage.

   RT_HOME/domains/IAMGovernanceDomain/jms/sharedtemp

> **Note:** Ensure that the directory location (*RT_HOME*/domains/IAMGovernanceDomain/jms/sharedtemp) specified for the BI JMS Shared directory, exists.

4. Update the JNDI URL as:

   cluster:t3://cluster_bi

5. Click **Apply**.

   Check the scheduler status in the **Scheduler Diagnostics** tab. The scheduler status must be **Passed**.

6. Click **Test JMS**.
7. Verify the above configurations on all the BI managed servers.
8. Restart all BI managed servers.

20.3 Validating BI Instance From the Web Tier

Validate the BI instance by accessing the following URL:

http://*igdadmin.example.com*/xmlpserver

Use the xelsysadm username and password to log in.

20.4 Verifying the Integration of BI Publisher with Oracle Identity Manager

To verify the integration of BI Publisher with Oracle Identity Manager in fresh configuration mode, do the following:

1. log in to the BI Publisher using your Oracle Identity Manager system administrator credentials by navigating to the following URL:

   http://*HOST_NAME*:*PORT*/xmlpserver

   The default port for BI Publisher server is 9704.

   > **Note:** Make sure that BI Publisher server is running when accessing the BI Publisher URL.

2. Click **Catalog**. The Oracle Identity Manager directory with reports is displayed under the **Shared Folders** directory.

You can now use the full capabilities of BI Publisher, such as PDF report generation and e-mail delivery.

> **Note:** In addition to the Oracle Identity Manager System administrator credentials, you can also access BI Publisher using the WebLogic credentials and the BISystemUser credentials.
>
> By default, BISystemUser password is same as that of the Oracle Identity Manager system administrator password.

20.5 Backing Up the Application Tier Configuration

It is recommended that you 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 information about database backups, see *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, back up the following:

- The Web tier
- The Access Manager database
- The Administration Server domain directory
- The Managed Server domain directory
- The LDAP Directory
- The Keystores created

20.6 Enabling Cluster-Level Session Replication Enhancements for Oracle BI Publisher

You can enable session replication enhancements for Managed Servers in a WebLogic cluster to which you deploy a Web application at a later time.

To enable session replication enhancements for `bi_cluster` in the domain IAMGovernanceDomain, use the values in Table 20–2.

Table 20–2 Network Channel Properties

Managed Server	Name	Protocol	Listen Address	Listen Port	Additional Channel Ports
WLS_BI1	`Replication Channel`	t3	OIMHOST1VHN3.example.com	7005	7006 to 7014
WLS_BI2	`Replication Channel`	t3	OIMHOST2VHN3.example.com	7005	7006 to 7014

Proceed as follows:

1. Log in to the WebLogic Administration console at:
   `http://IGDADMIN.example.com/console`
2. Ensure that Managed Servers in the `oim_cluster` cluster are up and running, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
3. To set replication ports for a Managed Server, use the values in Table 20–2.

   To set the values for `WLS_BI1`, for example, complete the following steps:

   a. Under **Domain Structure**, click **Environment** and **Servers**. The Summary of Servers page is displayed.

b. Click **Lock & Edit**.

c. Click `WLS_BI1` on the list of servers. The Settings for WLS_BI1 are displayed.

d. Click the **Cluster** tab.

e. In the **Replication Ports** field, enter a range of ports for configuring multiple replication channels. For example, replication channels for Managed Servers in `bi_cluster` can listen on ports starting from `7005` to `7015`. To specify this range of ports, enter `7005-7015`.

f. Repeat Steps **a** through **e** for each of the other managed servers in Table 20–2.

4. The following steps show how to create a network channel for the managed server WLS_BI1.

a. Log in to the Oracle WebLogic Server Administration Console.

b. If you have not already done so, click **Lock & Edit** in the Change Center.

c. In the left pane of the Console, expand **Environment** and select **Servers**.

The **Summary of Servers page** is displayed.

d. In the Servers table, click **WLS_BI1** Managed Server instance.

e. Select **Protocols**, and then **Channels**.

f. Click **New**.

g. Enter **ReplicationChannel** as the name of the new network channel and select **t3** as the protocol, then click **Next**.

h. Enter the following information:

Listen address: **OIMHOST1VHN1**

Note: This is the WLS_OIM1 floating IP assigned to WebLogic Server.

Listen port: **7005**

i. Click **Next**, and in the Network Channel Properties page, select **Enabled** and **Outbound Enabled**.

j. Click **Finish**.

k. Click **Save**.

l. Under the **Network Channels** table, select **ReplicationChannel**, the network channel you created for the WLS_BI1 Managed Server.

Expand **Advanced**, select **Enable SDP Protocol**, and click **Save**.

m. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

You must repeat the above steps to create a network channel each for the remaining Managed Servers in the cluster. Enter the required properties, as described in Table 20–2.

5. After creating the network channel for each of the Managed Servers in your cluster, click **Environment** > **Clusters**. The Summary of Clusters page is displayed.

6. Click **bi_cluster**. The Settings for bi_cluster page is displayed.

7. Click the **Replication** tab.
8. In the **Replication Channel** field, ensure that `ReplicationChannel` is set as the name of the channel to be used for replication traffic.
9. In the **Advanced** section, select the **Enable One Way RMI for Replication** option.
10. Click **Save**.
11. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

Complete this procedure for each domain.

21

Configuring Server Migration for an Enterprise Deployment

Configuring server migration allows Oracle Identity and Access Management-managed servers to be migrated from one host to another, so that if a node hosting one of the servers fails, the service can continue on another node. This chapter describes how to configure server migration for an Identity and Access Management enterprise deployment.

This chapter contains the following topics:

21.1 Overview of Server Migration for an Enterprise Deployment

Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_BI1, WLS_OIM2, WLS_SOA2, and WLS_BI2 Managed Servers. The WLS_OIM1, WLS_SOA1, and WLS_BI1 Managed Servers are configured to restart on OIMHOST2 should a failure occur. The WLS_OIM2, WLS_SOA2, and WLS_BI2 Managed Servers are configured to restart on OIMHOST1 should a failure occur. The WLS_OIM1, WLS_SOA1, WLS_BI1, WLS_OIM2, WLS_SOA2, and WLS_BI2 servers listen on specific floating IPs that are failed over by WebLogic Server Migration.

Perform the steps in the following sections configure server migration for the WLS_OIM1, WLS_SOA1, WLS_BI1, WLS_OIM2, WLS_SOA2, and WLS_BI2 Managed Servers.

21.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

In this section, you set up a user and tablespace for the server migration leasing table:

> **Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi data source for database leasing do not need to be re-created, but they must be retargeted to the clusters being configured with server migration.

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the sysdba user and run the following command:

```
create tablespace leasing
logging datafile
size 32m autoextend on;
```

> **Note:** This is an example where Oracle Managed Files is configured. If you are not using Oracle Managed Files, refer to your database administrator guide for information about creating a tablespace.

2. Create a user named `leasing` and assign to it the `leasing` tablespace:

```
create user leasing identified by password;
grant create table to leasing;
grant create session to leasing;
alter user leasing default tablespace leasing;
alter user leasing quota unlimited on leasing;
```

3. Create the `leasing` table using the `leasing.ddl` script:
   a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

```
WL_HOME/server/db/oracle/817
WL_HOME/server/db/oracle/920
```

   b. Connect to the database as the `leasing` user.
   c. Run the leasing.ddl script in SQL*Plus:

```
@Copy_Location/leasing.ddl;
```

   d. Currently, the script does not commit the change. Enter the following, at the SQL*Plus prompt, after the tool completes:

```
commit;
```

21.3 Creating a GridLink Data Source for Leasing Using the Oracle WebLogic Administration Console

In this section, you create a GridLink data source for the leasing table from the Oracle WebLogic Server Administration Console.

To create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.

3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
   - **Name**: Enter a logical name for the data source. For example, `leasing`.
   - **JNDI**: Enter a name for JNDI. For example, `jdbc/leasing`.
   - **Database Driver**: Select **For the Database Driver, select Oracle's Driver (Thin) for GridLink Connections Versions: 11 and later**.
   - Click **Next**.
5. In the Transaction Options page, de-select **Supports Global Transactions**, and click **Next**.
6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.
7. Enter the following connection properties:
   - **Service Name**: Enter the service name of the database (*`OIM_DB_SERVICENAME`*) with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example: `IGDEDG.example.com`
   - **Host Name and Port**: Enter the SCAN address a
     nd port for the RAC database being used. You can identify this address by querying the appropriate parameter in the database using the TCP Protocol:

     ```
     show parameter remote_listener;

     NAME                 TYPE        VALUE

     ------------------------------------------------

     remote_listener      string      IADDBSCAN.example.com:1521
     ```

     Note:

   - **Database User Name**: leasing
   - **Password**: For example: welcome1
   - **Confirm Password**: Enter the password again and click **Next**.
8. On the Test GridLink Database Connection page, review the connection parameters and click **Test All Listeners**. Here is an example of a successful connection notification:

   ```
   Connection test for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
   LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=IADDBSCAN.example.com)
   (PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=IGDEDG.example.com)) succeeded.
   ```

   where port 1521 is *DB_LSNR_PORT* and `oimedg.example.com` is *`OIM_DB_SERVICENAME`*.

   Click **Next**.
9. In the ONS Client Configuration page, do the following:
   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.

- Enter here also the SCAN address for the RAC database and the ONS remote port as reported by the database (example below) and click **ADD**:

  ```
  srvctl config nodeapps -s

  ONS exists: Local port 6100, remote port 6200, EM port 2016
  ```

- Click **Next**.

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

  ```
  IADDBHOST1.example.com (port 6200)
  ```

  and

  ```
  IADDBHOST2.example.com (port 6200)
  ```

  ---

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for IADDBSCAN.example.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select **oim_cluster**, **soa_cluster**, and **bi_cluster** as the targets, and **All Servers in the cluster**.
12. Click **Finish**.
13. Click **Activate Changes**.

21.4 Editing Node Manager's Properties File

In this section, you edit Node Manager's properties file. This must be done for the Node Managers on the nodes where the servers are running, OIMHOST1 and OIMHOST2.

The `nodemanager.properties` file is located in the following directory:

SHARED_CONFIG_DIR`/nodemanager/hostname.domain`

Add the following properties to enable server migration to work properly:

- `Interface:`

  ```
  Interface=bond0
  ```

  This property specifies the interface name for the floating IP. This will be `bond0` in most topologies. If external Oracle HTTP servers are being used, the managed servers will be listening on `bond1`. In that case, the `bond1` interface must be used here.

- `NetMask:`

  ```
  NetMask=255.255.254.0
  ```

  This property specifies the net mask for the interface for the floating IP. The net mask should the same as the net mask on the interface.

- UseMACBroadcast:

  UseMACBroadcast=true

  This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the -b flag in the arping command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
StateCheckInterval=500
bond0=*,NetMask=255.255.254.0
UseMACBroadcast=true
```

Note: The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. If not done already, set the StartScriptEnabled property in the nodemanager.properties file to true. This is required to enable Node Manager to start the managed servers.
2. Restart the Node Managers on OIMHOST1 and OIMHOST2 by running the startNodeManagerWrapper.sh script which is located in the *SHARED_CONFIG_DIR*/nodemanager/hostName.domain directory or use the procedure described in Section 31.1.4.1, "Starting Node Manager."

21.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

On Linux, you must set the environment and superuser privileges for the wlsifconfig.sh script. Perform this step on both OIMHOST1 and OIMHOST2.

Ensure that your PATH environment variable includes the files listed in Table 21–1.

Table 21–1 Files Required for the PATH Environment Variable

File	Located in this directory
wlsifconfig.sh	*IGD_MSERVER_HOME*/bin/server_migration
wlscontrol.sh	*WL_HOME*/common/bin
nodemanager.domains	*SHARED_CONFIG_DIR*/nodemanager/hostname.domain

Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.

For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform the following steps to set the environment and superuser privileges for the wlsifconfig.sh script.

Note: Ask the system administrator for the appropriate sudo and system rights to perform this step.

Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside `/etc/sudoers` granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`.

To grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

21.6 Configuring Server Migration Targets

In this section, you configure server migration targets. Configuring Cluster Migration sets the `DataSourceForAutomaticMigration` property to `true`.

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (**oim_cluster**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock and Edit**.
6. In the **Available** field, select the machines to which to allow migration, **OIMHOST1** and **OIMHOST2**, and click the right arrow.
7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
10. Select the server for which you want to configure migration.
11. Click the **Migration** tab.
12. Select **Automatic Server Migration Enabled** and click **Save**.
13. Click **Activate Changes**.
14. Repeat steps 2 through 13 for the SOA cluster and BI cluster.
15. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

21.7 Testing the Server Migration

In this section, you test that server migration is working properly.

The best way to validate server migration is to start Node Manager manually in a console window as described in Section 31.1.4.1, "Starting Node Manager."

To test from OIMHOST1:

1. Stop the WLS_OIM1 Managed Server. To do this, run this command:

   ```
   kill -9 pid
   ```

   where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

   ```
   ps -ef | grep WLS_OIM1
   ```

2. Watch the Node Manager terminal. You should see a message indicating that WLS_OIM1's floating IP has been disabled.
3. Wait for Node Manager to try a second restart of WLS_OIM1. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

To test from OIMHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart WLS_OIM1 on OIMHOST1, Node Manager on OIMHOST2 should prompt that the floating IP for WLS_OIM1 is being brought up and that the server is being restarted in this node.
2. Access the Oracle Identity Manager Console using the Virtual Host Name, for example: `http://OIMHOST1VHN.example.com:14000/identity`.

Follow the previous steps to test server migration for the WLS_OIM2, WLS_SOA1, and WLS_SOA2 Managed Servers.

Table 21–2 shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 21–2 Managed Server Migration

Managed Server	Migrated From	Migrated To
WLS_OIM1	OIMHOST1	OIMHOST2
WLS_OIM2	OIMHOST2	OIMHOST1
WLS_SOA1	OIMHOST1	OIMHOST2
WLS_SOA2	OIMHOST2	OIMHOST1
WLS_BI1	OIMHOST1	OIMHOST2
WLS_BI2	OIMHOST2	OIMHOST1

Verification From the WebLogic Administration Console:

Migration can also be verified in the Administration Console:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain at the address listed in Section 31.2, "About Identity and Access Management Console URLs."
2. Click **IAMGovernanceDomain** on the left pane.
3. Click the **Monitoring** tab and then the **Migration** sub tab.

   The Migration Status table provides information on the status of the migration.

Note: After a server is migrated, to fail it back to its original node/machine, stop the migrated Managed Server from the Oracle WebLogic Administration Console and see that the appropriate Node Manager starts the original Managed Server on the originally assigned machine.

21.8 Backing Up the Server Migration Configuration

Back up the database and the WebLogic domain, as described in Section 31.5.3, "Performing Backups During Installation and Configuration."

22

Configuring Single Sign-On

This chapter describes how to configure Single Sign-On for an Oracle Identity and Access manager enterprise deployment.

This chapter contains the following sections:

22.1 Overview of Configuring Single Sign-On

Configuring Single Sign-On requires the following tasks:

- Assign an LDAP group to the WebLogic Administration groups, if you have not already done so.
- Update the boot.properties file.
- Restart the servers.
- Install and configure WebGate and validate the setup.

After WebGate is installed and configured, the Oracle HTTP Server intercepts requests for the consoles and forwards them to Access Manager for validation.

The following administration consoles are referred to in this chapter:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console
- Oracle Access Management Console
- Oracle Access Manager Policy Manager
- Oracle Identity Manager System Administration Console
- Oracle Identity Manager Self Service Console

22.2 Configuring WebLogic Security Providers

When you run `configOAM` or `configOIM`, security providers will have been created in the domains IAMAccessDomain and IAMGovernanceDomain. These security providers will restrict access to the consoles in those domains based on the security policies of Oracle Access Manager. If you have other domains, create security providers in those domains manually. After creating the security providers, update them as described in the following sections.

Once you have enabled single sign-on for the administration consoles, ensure that at least one OAM Server is running to enable console access.

If you have used the Oracle Weblogic console to shut down all of the Access Manager Managed Servers, restart one of those Managed Servers manually before using the console again.

To start WLS_OAM1 manually, use the following command:

```
MSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://IADADMINVHN:7001
```

22.3 Updating the boot.properties File

Update the `boot.properties` file for the Administration Server and the managed servers with the WebLogic admin user created in Oracle Internet Directory.

You must update `boot.properties` on each administration server node. Follow the steps in the following sections to update the file.

This section contains the following topics:

Update the Administration Servers on All Domains

1. On each of the servers in the topology, go the directory:

   ```
   ASERVER_HOME/servers/serverName/security
   ```

   For example:

   ```
   cd IAD_ASERVER_HOME/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, start the server as soon as possible so that the entries get encrypted.

4. Restart the WebLogic Administration server and all managed servers.

22.4 Installing and Configuring WebGate for Oracle HTTP Server

This section describes how to install and configure WebGate for Oracle HTTP Server.

> **Note:** The instructions for installing and configuring WebGate differ depending on the web server you are using. If your web requests are being processed by Oracle HTTP server, then follow the steps described in Section 22.4, "Installing and Configuring WebGate for Oracle HTTP Server".
>
> If your web requests are being processed via Oracle Traffic Directory, then follow the steps described in Section 22.5, "Installing and Configuring WebGate for Oracle Traffic Director 11g".

This section contains the following topics:

- Section 22.4.1, "Installing Oracle WebGate on WEBHOST1 and WEBHOST2"
- Section 22.4.2, "Deploying WebGate to WEBHOST1 and WEBHOST2"

22.4.1 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before starting the installer ensure that Java is installed on your machine.

1. Start the WebGate installer by issuing the command:

   REPOS_HOME/installers/webgate/Disk1/runInstaller

   You are asked to specify the location of the Java Development Kit for example:

   REPOS_HOME/jdk

2. On the Welcome screen, click **Next**.
3. On the Install Software Updates Screen, choose whether to install software updates and if necessary, enter your myoraclesupport credentials and click **Next**.
4. On the Prerequisites screen, after all the checks have successfully completed, click **Next**.
5. On the Installation Location Screen, enter the following information:
   - **Oracle Middleware Home**: *WEB_MW_HOME*
   - **Oracle Home Directory**: webgate_ohs

     WEB_MW_HOME/webgate_ohs is defined as *WEBGATE_ORACLE_HOME*

   Click **Next**.
6. On the Installation Summary screen, click **Install**.
7. Click **Next**.
8. Click **Finish**.

22.4.2 Deploying WebGate to WEBHOST1 and WEBHOST2

To deploy WebGate to WEBHOST1 and WEBHOST2:

1. Execute the command deployWebGate which is located in:

WEBGATE_ORACLE_HOME/webgate/ohs/tools/deployWebGate

The command takes the following arguments:

Oracle HTTP Instance configuration Directory

WebGate Home Directory

For example:

```
./deployWebGateInstance.sh -w OHS_ORACLE_INSTANCE/config/OHS/ohs1 -oh  WEBGATE_
ORACLE_HOME
```

2. Set the library path and change directory.

   Set the library path to include the *WEB_ORACLE_HOME*/lib directory, for example:

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
   ```

   Change directory:

   WEBGATE_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools

3. Run the following command to copy the file apache_webgate.template from the WebGate home directory to the WebGate instance location (renamed to webgate.conf) and update the httpd.conf file to add one line to include the name of webgate.conf.

   ```
   ./EditHttpConf -w OHS_ORACLE_INSTANCE/config/OHS/ohs1 -oh WEBGATE_ORACLE_HOME
   ```

4. Copy the files ObAccessClient.xml and password.xml, which were generated when you created the agent from the directory *IAD_ASERVER_HOME*/output/Webgate_IDM_11g on OAMHOST1, to the directory *OHS_ORACLE_INSTANCE*/config/OHS/ohs1/webgate/config.

5. Copy the directory wallet, which was generated when you created the agent from the directory *IAD_ASERVER_HOME*/output/Webgate_IDM_11g on OAMHOST1, to the directory *OHS_ORACLE_INSTANCE*/config/OHS/ohs1/webgate/config.

6. Copy the files aaa_key.pem and aaa_cert.pem which were generated when you created the agent from the directory *IAD_ASERVER_HOME*/output/Webgate_IDM_11g to the WebGate instance directory *OHS_ORACLE_INSTANCE*/config/OHS/ohs1/webgate/config/simple.

7. Restart the Oracle HTTP Servers.

22.5 Installing and Configuring WebGate for Oracle Traffic Director 11*g*

This section describes how to install and configure WebGate.

Note: The instructions for installing and configuring WebGate differ depending on the web server you are using. If your web requests are being processed by Oracle HTTP server, then follow the steps described in Section 22.4, "Installing and Configuring WebGate for Oracle HTTP Server".

If your web requests are being processed via Oracle Traffic Directory, then follow the steps described in Section 22.5, "Installing and Configuring WebGate for Oracle Traffic Director 11g".

This section contains the following topics:

22.5.1 Prerequisites

Install and configure the Oracle Traffic Director as described in Section 14.2, "Configuring Oracle Traffic Director," before installing the Oracle Web Gate:

22.5.2 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before starting the installer ensure that Java is installed on your machine. To install Oracle WebGate, complete the following steps on WEBHOST1 and WEBHOST2. The WebGate installer can be found in the directory *REPOS_HOME*/installers/webgate_otd.

> **Note:** If your web hosts are using shared storage for the OTD binaries, you must install WebGate on one of these hosts only.

1. Start the WebGate installer by issuing the command:

   ```
   ./runInstaller
   ```

   You are asked to specify the location of the Java Development Kit for example:

   WEB_MW_HOME/jdk

2. On the Welcome screen, click **Next**.
3. On the Install Software Updates screen, choose whether to skip updates, check with Oracle Support for updates, or search for updates locally.

   Click **Next**.
4. 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**.
5. If the prerequisites fail because of missing 32-bit libraries, you can safely ignore this failure.
6. Click **Next**.
7. On the Installation Location Screen, enter the following information:

   Oracle Middleware Home: *WEB_MW_HOME*

   Oracle Home Directory: *webgate_otd*

   Click **Next**.
8. On the installation summary screen, click **Install**.

9. Click **Next**.
10. Click **Finish**.
11. Execute the `deployWebGateInstance.sh` command from the following directory:

    OTD_WEBGATE_ORACLE_HOME`/webgate/iplanet/tools/deployWebGate`

    Make sure this tool has executable permission.

    For example:

    ```
    cd OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/tools/deployWebGate
    ./deployWebGateInstance.sh -w LOCAL_CONFIG_DIR/instances/webgate_otd/webgate/
    -oh OTD_WEBGATE_ORACLE_HOME -ws otd
    ```

    Expected output:

    ```
    Copying files from WebGate Oracle Home to WebGate Instancedir
    ```

    Note: The deployment and instance directory must be the same on every host.

12. Set the environment variable `LD_LIBRARY_PATH` to *OTD_WEBGATE_ORACLE_HOME*`/webgate/iplanet/lib` using the following command:

    ```
    export LD_LIBRARY_PATH=OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/lib
    ```

13. Add the WebGate properties to each of the property files for your OTD virtual hosts. These are located in the directory *LOCAL_CONFIG_DIR*`/net-login.example.com/config` where *login.example.com* is the name of the OTD configuration you specified in Section 14.2.3, "Creating a Configuration".

    The virtual host files names will depend on the values of your virtual hosts. In this book, the files are called:

    - login.example.com-obj.conf
    - prov.example.com-obj.conf
    - iadadmin.example.com-obj.conf
    - igdadmin.example.com-obj.conf
    - iadinternal.example.com-obj.conf
    - igdinternal.example.com-obj.com

    To do this, perform the following steps for each of the files:

    1. Change your present working directory to *OTD_WEBGATE_ORACLE_HOME*`/webgate/iplanet/tools/setup/InstallTools`.
    2. Run the following command:

       `./EditObjConf -f` *config_file* `-oh` *OTD_WEBGATE_ORACLE_HOME* `-w` *instance_directory* `-ws otd`

       For example:

       ```
       ./EditObjConf -f OTD_ORACLE_INSTANCE/net-login.example.com/config/login.example.com-obj.conf -oh OTD_WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd
       ```

Note: It is optional to run this command for igdinternal and iadinternal. These URLs are accessible only inside the Exalogic rack. Therefore, it is unlikely that unauthenticated requests will be accessing them. Adding WebGate to these virtual hosts can slow internal callbacks. If not added, it is marginally less secure. So, if you insist on maximum security, add them as described earlier.

If you installed OTD to run as root, then you will have to run these commands as root.

The following is a sample output:

```
OTD_ORACLE_INSTANCE/config/magnus.conf has been backed up as OTD_ORACLE_
INSTANCE/config/magnus.conf.ORIG
OTD_ORACLE_INSTANCE/config/instance_config_name-obj.conf has been backed up
as
OTD_ORACLE_INSTANCE/instance_config_name-obj.conf.ORIG
```

14. Edit the properties in the `login.example.com-obj.conf` and `admin.example.com-obj.conf` files using the `EditObjConf` tool located in the following directory:

```
OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/tools/setup/InstallTools
```

For example, on WEBHOST1, run the following:

```
./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/login.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd

./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/prov.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd

./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/iadadmin.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd

./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/igdadmin.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd

./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/igdinternal.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd

./EditObjConf -f OTD_ORACLE_
INSTANCE/net-login.example.com/config/iadinternal.example.com-obj.conf -oh OTD_
WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/instances/webgate_otd -ws otd
```

Note: If you installed OTD to run as `root`, then you must run these commands as `root`.

It is optional to run this command for `igdinternal` and `iadinternal`. These URLs are accessible only inside the Exalogic rack. Therefore, it is unlikely that unauthenticated requests will be accessing them. Adding WebGate to these virtual hosts can slow internal callbacks. If not added, it is marginally less secure. So, if you insist on maximum security, add them as described earlier.

Expected output:

```
OTD_ORACLE_INSTANCE/config/magnus.conf has been backed up as OTD_ORACLE_
INSTANCE/config/magnus.conf.ORIG
OTD_ORACLE_INSTANCE/config/instance_config_name-obj.conf has been backed up as
OTD_ORACLE_INSTANCE/instance_config_name-obj.conf.ORIG
```

15. Register WebGate to the Access Manager 11g Server by copying the WebGate artifacts Located in the following directory:

    ```
    IAD_ASERVER_HOME/output/Webgate_IDM_11g
    ```

    to the following directories.

    Copy `aaa_cert.pem` and `aaa_key.pem` to:

    ```
    LOCAL_CONFIG_DIR/instances/webgate_otd/webgate/config/simple
    ```

    Copy `cwallet.sso`, `ObAccessClient.xml`, and `password.xml` to:

    ```
    LOCAL_CONFIG_DIR/instances/webgate_otd/webgate/config
    ```

    To copy the artifacts run the following commands:

    ```
    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/aaa* to LOCAL_CONFIG_
    DIR/instances/webgate_otd/webgate/config/simple

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/password.xml to LOCAL_CONFIG_
    DIR/instances/webgate_otd/webgate/config/

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/ObAccessClient.xml to LOCAL_CONFIG_
    DIR/instances/webgate_otd/webgate/config/

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/cwallet.sso to LOCAL_CONFIG_
    DIR/instances/webgate_otd/webgate/config/
    ```

    Note: If you have performed your installation using IDMLCM, you must copy the files from the deployed OHS instance. For example:

    ```
    LOCAL_CONFIG_
    DIR/instances/ohs1/config/OHS/ohs1/webgate/config
    ```

    ---

16. Repeat the steps 11 through 15 for each of the WEBHOSTs.

Note: Configuring WebGate in this way directly modifies the Oracle Traffic Director configuration files. These changes are not reflected in the OTD configuration store. The next time you go into OTD and modify the configuration, OTD it will indicate that there is a discrepancy between that config store and the values on disk. It will ask you what you want to do. YOU MUST tell OTD to pull the configuration from the files rather than push the configuration back to the files. Selecting the wrong option will remove the WebGate configuration you just performed.

22.5.3 Adding LD_LIBRARY_PATH to OTD Start Scripts

To prevent you having to enter the `LD_LIBRARY_PATH` each time you start OTD, you can add it to the OTD start script.

To do this, proceed as follows:

Note: If you installed OTD to run as `root`, then you must perform these steps as `root` user.

1. Edit the file `startserv`, which is located in the directory: *`WEB_ORACLE_INSTANCE`*`/net-`*`login.example.com`*`/bin`
2. Locate the line that looks like this:

```
# Set LD_LIBRARY_PATH for Solaris and Linux
LD_LIBRARY_PATH="${SERVER_LIB_PATH}:${LD_LIBRARY_PATH}"; export LD_LIBRARY_PATH
```

3. Add the following line afterwards:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/lib;
export LD_LIBRARY_PATH
```

4. Save the file.

22.5.4 Restarting the Oracle Traffic Director Instance

Use the `startserv` command to start or `stopserv` command to stop your Oracle Traffic Director instance.

If you did not install Oracle Traffic Director as root. Stop the failover groups using the following command as root:

```
OTD_ORACLE_HOME/bin/tadm stop-failover --instance-home=OTD_ORACLE_INSTANCE/
--config=login.example.com
```

To stop the server, run the following command:

```
OTD_ORACLE_INSTANCE/net-login.example.com/bin/stopserv
```

To start the server, run the following command:

```
OTD_ORACLE_INSTANCE/net-login.example.com/bin/startserv
```

If you did not install Oracle Traffic Director as root. Start the failover groups using the following command as root:

```
OTD_ORACLE_HOME/bin/tadm start-failover --instance-home=OTD_ORACLE_INSTANCE/
--config=login.example.com
```

To restart the Oracle Traffic Director instance, stop all running instances, and then run the start command.

22.5.5 Updating OTD Configuration Repository with WebGate Changes

The commands in previous sections manually update the Oracle Traffic Director configuration files. After the files are updated, the OTD configuration is inconsistent with the information in the files. Subsequent deployments would therefore erase the new configuration. Therefore, you must update the OTD configuration with the manual changes made in the previous sections.

To update the OTD configuration:

1. Log in to the OTD Administration Console using the following URL:

   `https://OTDADMINVHN:OTD_ADMIN_PORT`

2. Click the **Deploy** button at the top of the screen.

   A message box appears stating that the administration server has detected configuration modifications on some instances.

3. Select the option **Pull and deploy configuration** and click **OK**.

22.6 Validating Oracle Access Management Single Sign-On Setup

To validate that WebGate is functioning correctly, open a web browser and go the Access Management Console URL listed in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

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

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console and to Oracle Enterprise Manager Fusion Middleware Control at the URLs listed in Section 31.2, "About Identity and Access Management Console URLs."

The Oracle Access Management Single Sign-On page displays. Provide the credentials for the `weblogic_idm` user to log in.

Part IV

Configuring an Enterprise Deployment Using Life Cycle Management (LCM) Tools

Use this part of the guide to automatically deploy the Oracle Identity and Access Management software using the Life Cycle Management (LCM) Tools.

This part contains the following chapters:

23

Introduction to the Life Cycle Management (LCM) Tools

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

This chapter contains the following sections:

23.1 About the Automated Deployment of Oracle Identity and Access Management

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

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

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

For information about using the LCM Tools to deploy Oracle Identity and Access Management on a single host, see the *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

This chapter, and the following chapters, provide instructions on how to use the LCM Tools in a multi-node, enterprise deployment environment.

You can use the LCM tools as an alternative to the manual installation and configuration steps provided in Part III, "Configuring an Oracle Identity and Access Management Enterprise Deployment Manually".

23.1.2 Packaging and Distribution of the Automation Tools

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

Note: If you are deploying Oracle Identity and Access Management on the Exalogic engineered system, then you will need to download additional software packages for Oracle Traffic Director and Oracle Access Manager WebGate for Oracle Traffic Director.

For more information, see Section 5.4, "Identifying and Obtaining Software Downloads for an Enterprise Deployment".

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

For more informations, see Section 7.5.5.1, "Life Cycle Management and Deployment Repository".

23.1.3 Obtaining and Applying Required Patches

Before you begin using the LCM Tools to automate your Oracle Identity and Access Management deployment, be sure to download the latest patches to both the Oracle Identity and Access Management software and the LCM Tools.

For more information, see "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Identity and Access Management Release Notes*.

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

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

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

  Note that this guide describes how to use the LCM Tools to deploy a limited number of specific Oracle Identity and Access Management topologies. For more information, see Section 2.2, "Diagrams of the Primary Oracle Identity and Access Management Topology" and Section 3.3, "Diagrams of the Primary Oracle Identity and Access Management Exalogic Enterprise Topologies".

- The Oracle Identity and Access Management software and the required components such as the Java Development Kit (JDK), Oracle WebLogic Server, Oracle HTTP Server, and Oracle SOA Suite are packaged into a single repository

that can be downloaded from the Oracle Technology Network (OTN) or the Oracle Software Delivery Cloud.

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

For more information, see Section 5.4, "Identifying and Obtaining Software Downloads for an Enterprise Deployment".

- When you are deploying to multiple hosts, you can run the LCM Tools from a single host. The scripts execute the necessary operations on the local host and on the remote hosts. There is no need to run the LCM Tools manually on each host.
- The LCM Tools use the Environment Health Check Utility to verify that your system requirements before you deploy and to verify the environment after you deploy.

  For more information, see *Verifying Your Oracle Identity and Access Management Environment*.
- The environment you deploy using the LCM tools can later be upgraded component by component, so as to minimize downtime.

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

  For more information, see the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.
- You can use the LCM Tools to deploy an Oracle Identity and Access Management environment that uses an existing Microsoft Active Directory instance. For more information, see Section 13.6, "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management".
- When you deploy on a consolidated topology, the LCM tools creates the Access and Governance Administration Servers on the same host. The topology diagrams depict them on different hosts to spread the load. If you wish to have your Administration Servers on different hosts per the topology diagrams, then let the LCM configure both Administration Servers on IAMHOST1. After provisioning is complete, you can then fail one of the Administration Servers over to IAMHOST2 using the procedure described in Section 15.4.11, "Manually Failing over the WebLogic Administration Server".

Note: You cannot change the IDMLCM response file name if you are updating an existing file.

Limitations of Using the LCM Tool

The current LCM implementation has the following limitations:

- Installing and creating an Oracle Directory is not supported. You must create the Oracle Unified Directory (OUD) or Oracle Internet Directory (OID) using the manual steps prior to running a deployment.

  For more information, see Chapter 12, "Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment".

- If you plan to perform an incremental deployment, where you first deploy and validate Oracle Access Manager or Oracle Identity Manager, and later deploy the other product, note the following:

  Oracle Access Manager Only and Oracle Identify Manager Only topologies cannot use the same IDM_TOP. If you wish to perform such a modular installation using OAM Only and OIM Only, then you must specify a different IDM_TOP for each install.

  This means creating two different mount points and additional shared storage. Another approach is to use LCM to create the first deployment; for example, OAM only, and then Install the second, OIM Only, deployment using the manual steps. If this is done, then the same IDM_TOP can be used.

- The Cleanup and Restore feature is supported only for single-host deployments. For more information, see Chapter 28, "Cleaning up an Environment Before Rerunning IAM Deployment".
- Scale out and scale up of a configured environment is not automated by the LCM Tools. For more information, see Chapter 29, "Scaling Enterprise Deployments".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 23–1 describes each of the steps and provides links to more information about each step.

Table 23–1 Roadmap for Creating the Reference Topologies with the LCM Tools

Task	Description	More Information
Determine the topology you want to deploy	Review the topologies supported by the LCM Tools and determine which topology is best suited for the requirements of your organization. The following are the topologies supported: ▪ Oracle Identity Manager (OIM) Only ▪ Oracle Access Manager (OAM) Only ▪ OIM-OAM-OMSS Integrated with Directory	Chapter 2, "Understanding the IAM Enterprise Deployment" Chapter 3, "Understanding the IAM Exalogic Enterprise Deployment"
Review the certifications and system requirements.	Before you install and configure Oracle Identity and Access Management, you should ensure that your existing products are certified for use with Oracle Identity and Access Management. In addition, you should review the system requirements, such as memory and disk space requirements and required Linux install packages.	Chapter 5, "Procuring Resources for an Enterprise Deployment"
Review the IDM and LCM readmes.	After you apply the required patches, review the bundle patch readmes to determine for instructions about applying the patches and preparing the software for deployment.	Section 23.1.3, "Obtaining and Applying Required Patches"

Table 23–1 (Cont.) Roadmap for Creating the Reference Topologies with the LCM Tools

Task	Description	More Information
Perform the standard planning, procurement, and configuration procedures to prepare for the enterprise deployment.	A database is required to store the required schemas for the Oracle Identity and Access Management products and components. You can identify an existing database instance, or use the database installation software included in the repository to install a new database.	Part II, "Preparing for an Enterprise Deployment"
Run the Health Check Utility to ensure your certification and system requirements have been met.	This step ensures that you can run the Deployment Wizard and the basic and mandatory system requirements have been met.	"Running the Health Check Utility to Verify Basic System Requirements" in the *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*
Determine the LDAP Directory requirements for the topology you selected	Some of the supported topologies require a supported LDAP directory service. If you plan to use an existing directory service, there are tasks you must perform to prepare the directory for use with Oracle Identity and Access Management.	Chapter 12, "Configuring Oracle LDAP for an Identity and Access Manager Enterprise Deployment"
Download and unpack the LCM Tools and Repository from the Oracle Technology Network (OTN) or the Software Delivery Cloud	When you unpack the archives, you end up with a standard directory structure that includes a software repository. The software repository contains all the installers required to install the Oracle Identity and Access Management software, as well as the installer for installing the LCM Tools. Note that the latest version of the LCM tool set is delivered as a patch which is an independent download.	Section 5.4, "Identifying and Obtaining Software Downloads for an Enterprise Deployment"
Install the LCM Tools	From the software repository, locate and run the LCM Tools installer, which installs the provisioning tools that enable you to automatically deploy Oracle Identity and Access Management.	Chapter 24, "Installing Oracle Identity and Access Management Life Cycle Management Tools"
Run the Deployment Wizard to create a new deployment response file.	The Deployment Wizard (one of the LCM Tools), prompts you for important information about your hardware and software environment, such as the selected topology, database, and LDAP directory information. The wizard uses this information to create a response file that can later be used to automatically deploy Oracle Identity and Access Management.	Chapter 25, "Creating a Deployment Response File"
Run the Deployment Wizard or the command line to deploy the Oracle Identity Management software.	For this step, you use the response file (which now contains all the details about your hardware and software environment) to deploy the Oracle Identity and Access Management software automatically.	Chapter 26, "Deploying Identity and Access Management"

24

Installing Oracle Identity and Access Management Life Cycle Management Tools

This chapter describes how to install the Oracle Identity and Access Management Life Cycle Management (LCM) Tools.

The provisioning file created as a result of running the IAM deployment wizard must be visible to each host in the same location during provisioning and subsequent patching.

For information about obtaining the software, see Section 5.4, "Identifying and Obtaining Software Downloads for an Enterprise Deployment".

This chapter contains the following topics:

- Section 24.1, "About the Deployment Repository and LCM Tools Directory Structure"
- Section 24.2, "Locating the Required Java Development Kit (JDK)"
- Section 24.3, "Installing the Oracle Identity and Access Management Life Cycle Tools"

24.1 About the Deployment Repository and LCM Tools Directory Structure

When you unpack the downloadable archives for the Oracle Identity and Access Management Deployment Repository into *REPOS_HOME*, the directory structure looks similar to the one illustrated in Figure 7–1, "Deployment Repository".

Table 24–1 describes each of these key directories, their purpose and how they get created.

For more information about using the Deployment Wizard to create the response file, see Chapter 25, "Creating a Deployment Response File".

Table 24–1 Key Directories Used by the LCM Tools

Directory	Purpose	When Created	Where to Specify During Install and Deployment
REPOS_HOME	Contains the required Java Development Kit (JDK) and all the product installers required to install and configure Oracle Identity Management.	This directory is created when you unpack the Repository archives from the Oracle Technology Network (OTN).	Enter the value of the REPOS_HOME in the **Software Repository Location** field of the Deployment Wizard when you are creating a response file.

Table 24–1 (Cont.) Key Directories Used by the LCM Tools

Directory	Purpose	When Created	Where to Specify During Install and Deployment
IDMLCM_HOME	Oracle home for the LCM Tools. From this directory structure, you run the LCM Deployment Wizard.	This directory is created by the LCM Tools installer.	Enter in the **Oracle Home Directory** field in the IDM LCM Tools Installer.
IDM_TOP	Top-level directory for the Oracle Identity and Access Management environment. It consists of: ■ **`IDM_TOP/products`**, which contains the software binaries ■ **`IDM_TOP/config`**, which contains the domains, instances, and other runtime artifacts	The IDM_TOP directory, as well as its subdirectories, are created by the LCM Tools during the deployment of the Oracle Identity Management software.	In the Deployment Wizard, when creating the response file: ■ Enter the location of IDM_TOP in the **Software Installation Location** field. ■ Enter the location of the `config` directory in the **Shared Configuration Location** field. **Note:** The configuration location is set to a location inside the IDM_TOP directory by default; however, you can have the Deployment Wizard create the directory in any accessible location. The `products` directory will be created inside the IDM_TOP directory when you deploy the software.

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

```
chmod -R 755 *
```

24.2 Locating the Required Java Development Kit (JDK)

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

`REPOS_HOME``/jdk`

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

24.3 Installing the Oracle Identity and Access Management Life Cycle Tools

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

For more information, see the following topics:

- Section 24.3.1, "Locating and Starting the LCM Tools Installer"
- Section 24.3.2, "Summary of the LCM Tools Installer Screens"
- Section 24.3.3, "Specifying an Inventory Directory"
- Section 24.3.4, "Applying the Patch for LCM Tools"

24.3.1 Locating and Starting the LCM Tools Installer

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

REPOS_HOME/installers/idmlcm/Disk1

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

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

On UNIX:

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

For example:

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

24.3.2 Summary of the LCM Tools Installer Screens

Table 24–2 describes each of the LCM Tools installer screens.

Table 24–2 Installation Flow for Oracle Identity and Access Management LCM Tools

Screen	Description and Action Required
Welcome	Review the information on the Welcome page, and click **Next**.
Specify Inventory Directory	This screen appears if this is the first time you are installing Oracle software on a UNIX host or if you installed software previously on the UNIX host, but did not create a central inventory. The Inventory Directory is used to keep track of all Oracle products installed on this host. For the purposes of this guide: 1. Click **OK** to accept the default location of the Inventory Directory and the default Operating System Group Name for the directory. 2. In the Inventory Location Confirmation dialog box, select **Continue Installation with local inventory**. If you want to create a central Inventory Directory or learn about the advantages of doing so, see Section 24.3.3, "Specifying an Inventory Directory".

Table 24–2 (Cont.) Installation Flow for Oracle Identity and Access Management LCM

Screen	Description and Action Required
Install Software Updates	If you wish to search for and download software updates from My Oracle Support, do the following: 1. Select **Search My Oracle Support for Updates**. 2. Enter **User name** and **Password**. 3. Click **Test Connection**. If you wish to search your local directory for updates, do the following: 1. Select **Search Local Directory for Updates**. 2. Click **Search For Updates**. If you wish to skip software updates, select **Skip Software Updates**. Click **Next** to continue.
Prerequisite Checks	On this screen, verify that checks complete successfully, then click **Next**.

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

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

24.3.3 Specifying an Inventory Directory

If you are running on a UNIX platform, and you have not previously installed an Oracle product on this host, or if you installed software previously on the UNIX host, but did not create a central inventory, then the Specify Inventory Directory screen will appear during the installation.

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

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

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

To create a central inventory directory:

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

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

   Click **OK** to continue.

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

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

   `inventory_loc=`*`path_to_central_inventory`*

   `inst_group=`*`install_group`*

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

24.3.4 Applying the Patch for LCM Tools

After you install the LCM Tools, locate and apply the latest LCM Tools patch. For more information, see "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes for Identity Management* for 11*g* Release 2 (11.1.2.3.0).

For instructions on applying the patch, refer to the README file which is included with the patch.

25

Creating a Deployment Response File

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

This chapter contains the following sections:

25.1 What is a Deployment Response File?

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

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

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

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

The tool creates the following three types of response files:

- Oracle Identity Manager (OIM) Only - Use this option for implementations that will contain only the IAM Identity Governance components.
- Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Only - Use this option for implementations that will contain only the IAM Access components.
- OIM - OAM - OMSS Integrated with Directory - Use this option for implementations that will contain both Identity Governance and Access components.

Note: "Oracle Access Manager (OAM) and Oracle Mobile Security Suite (OMSS) Only", and "OIM - OAM - OMSS Integrated with Directory" solutions require that an existing LDAP directory be present.

If your directory is OUD or OID, the deployment tool can prepare the directory for you, or you can prepare it yourself using the steps in the manual sections of this guide.

If your directory is Active Directory, you need to prepare the directory manually using the instructions described in Section 13.6, "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management".

IDMLCM does not support the update of RSP file with a different name. If you want to update the RSP file, you must save the file with same name with which it was created.

If you are performing a modular deployment, for example, starting off with OAM, and if you wish to add OIM later, then you should first create a response file for OAM only, and follow the steps to deploy it. Then at a later time, create a deployment file for OIM only, and follow the steps to deploy that. When you have performed the second deployment, you will have to integrate the two component together manually. If this is your long term goal (using OAM and OIM together), then when configuring OIM only, you should choose to enable LDAPSYNC. If you do not do so, then extra manual steps will be required to enable that. Steps to do this are not covered in this guide.

25.2 Starting the Deployment Wizard and Navigating the Common Screens

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

   For more information, see Section 24.2, "Locating the Required Java Development Kit (JDK)".

2. Start the Deployment Wizard:

   a. Change directory to the following directory:

      IDMLCM_HOME/provisioning/bin

      In this example, *IDMLCM_HOME* is the directory where you installed the LCM Tools. For more information, see Section 24.1, "About the Deployment Repository and LCM Tools Directory Structure".

   b. Enter the following command:

      ```
      ./iamDeploymentWizard.sh
      ```

3. Review the Welcome screen to learn more about the Deployment wizard and to review the prerequisites. Click **Next**.

4. If the Specify Inventory Directory screen appears:

   a. Click **OK** to accept the default location of the central inventory directory and the default Operating System Group Name for the directory.

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

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

If you want to create a central inventory directory or learn about the advantages of doing so, see Section 24.3.3, "Specifying an Inventory Directory".

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

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

   After you enter the required information, click **Next**.
8. Depending on the Oracle Identity and Access Management topology you're deploying, proceed to the appropriate section:
   - Section 25.3, "Creating a Deployment Response File for Oracle Identity Manager (OIM) Only Topology"
   - Section 25.4, "Creating a Deployment Response File for Oracle Access Manager (OAM) Only Topology"
   - Section 25.5, "Creating a Deployment Response File for a Fully Integrated Topology"

Note: Use the *Enterprise Deployment Workbook for Identity Management* to help you complete the information in the following sections.

If you are deploying on Exalogic, for host names, use the name of the host as derived from the hostname command in the topology screens.

25.3 Creating a Deployment Response File for Oracle Identity Manager (OIM) Only Topology

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

1. Ensure that you have completed the steps described in Section 25.2, "Starting the Deployment Wizard and Navigating the Common Screens".
2. On the Suite Selection screen, select **Oracle Identity Manager (OIM) Only**.

   Select **Enable LDAP Sync** if you are integrating Oracle Identity Manager with an LDAP directory. LDAP sync synchronizes users created in OIM with users created in LDAP. If you are planning to integrate OAM with OIM, then this value should be set to true. This can be enabled post deployment, but is outside the scope of this guide.

   > **Note:** After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection. If you need to make any modification in the previous screens, click **Cancel** and then restart the Oracle Identity and Access Management Deployment Wizard.

   Click **Next**.
3. On the Directory Selection screen, choose the type of directory you wish to synchronize OIM with. This screen appears only if you selected **Enable LDAP Sync**. The following are the valid types of directories:

   - Oracle Unified Directory
   - Oracle Internet Directory
   - Microsoft Active Directory

   > **Note:** If you are using Active Directory, you must prepare the directory before running the deployment wizard, using the instructions described in Section 13.6, "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management".

   Click **Next**.
4. On the Select Topology screen, select **Highly Available (HA)**.

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

   For example:

   First Instances:

   Identity and Governance: oimhost1.example.com

   Web Tier: webhost1.example.com

   Second Instances:

   Identity and Governance: oimhost2.example.com

Web Tier: webhost2.example.com

> **Note:** On a multi-networked host, the host name entered (without the domain) must be same as the result returned from the `hostname` command issued on the machine.
>
> If you have multiple network cards and if you wish to provision using one other than that attached to the default hostname for the duration of provisioning, you must set the hosts hostname to that associated with the value you enter here. This is particularly important on Exalogic Deployments.

Click **Next**.

5. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions. For more information about directory locations, see Chapter 7, "Preparing Storage for an Enterprise Deployment".

   The following are the fields on this screen:

   - **Lifecycle Management Store Location**: *LCM_HOME*
   - **Mounted on Webhosts**: Select this option if *LCM_HOME* directory needs to be mounted on WEBHOST1 and WEBHOST2 during installation. This is the recommended approach.
   - **Software Repository Home**: *REPOS_HOME*
   - **Software Installation Location**: *IDM_TOP*
   - **Shared Configuration Location**: *SHARED_CONFIG_DIR*
   - **Local Configuration Location**: *LOCAL_CONFIG_DIR*

   > **Note:** If you have already run the deployment tool to create a deployment and you wish to run it again to create a second deployment; for example, if you have run the tool for OAM Only and are now running the tool again for OIM Only, the Software Installation Location MUST be different for each installation, whereas the configuration directories can be the same. This is a limitation in this version of the deployment tool.

   Click **Next**.

6. Use the Configure Virtual Hosts screen to enter the virtual host names used by each component. For example:

   Identity Governance Domain Admin Server: `idgadminvhn.example.com`

   SOA Server 1: `oimhost1vhn2.example.com`

   SOA Server 2: `oimhost2vhn2.example.com`

   OIM Server 1: `oimhost1vhn1.example.com`

   OIM Server 2: `oimhost2vhn1.example.com`

   BIP Server 1: `oimhost1vhn3.example.com`

   BIP Server 2: `oimhost2vhn3.example.com`

Click **Next**.

7. On the Directory Configuration screen, enter the details of the directory where OIM stores the user and Group information when syncing to LDAP. This section appears only if you enabled LDAP Sync. The following fields are present on this screen:

   - **Directory Host**: This is the host name of the directory. In the case of a highly available setup, this is the directory load balancer entry point. For example, `idstore.example.com`
   - **Directory Port**: This is the LDAP directory port. In the case of a highly available setup, this is the port on the Load Balancer, that is, *`LBR_LDAP_PORT`* from the worksheet.
   - **Administrator**: This is the LDAP administrator account. For example, `cn=oudadmin`
   - **Administrator Password**: The LDAP administrator password (*`LDAP_ADMIN_USER`*)
   - **Realm DN**: This is the area in the LDAP directory where users and groups are created (*`REALM_DN`*).
   - **Users Container**: This is the location in the LDAP directory where users are held (*`USERS_CONTAINER`*).
   - **Groups Container**: This is the location in the LDAP directory where groups are held (*`GROUPS_CONTAINER`*).

   Click **Next** to continue.

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

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

   Click **Next** to continue.

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

   Set the **Location of the JMS/Tlogs** to the shared storage location where you are placing runtime artifacts. For example:

   `RT_HOME``/domains/IAMGovernanceDomain`

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

   Select **Configure Email Server** if you want to identify and configure a mail server so that Oracle Identity Manager can send email notifications. If you wish to configure the Email Server, you must to provide the following information:

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

- **Username**: This is username (`EMAIL_USER`) you use to authenticate with the Email server.
- **Password**: This is the password (`EMAIL_PASSWORD`) for the above user.
- **Web Proxy Host**: This is the port of your proxy server if you use one.
- **Web Proxy Port**: This is the host name of your proxy server if you use one.

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

    If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do not select the **Create Schema Using RCU** check box. In this case, you must provide the required information to connect to the database where the schemas are installed:

    If you have not installed the schemas already, then select **Create Schema Using RCU**. If you choose this option, the LCM Tool creates the schemas as part of the deployment process.

    The following fields are present in this screen:

    - **SYSDBA Username**: This is the name of the SYSDBA account on the database. For example, `sys`
    - **SYSDBA Password**: This is the password for the SYSDBA account.

      SYSDBA credentials are required only if you select **Create Schema Using RCU** option.
    - **Schema Prefix**: This is the prefix that was used when you created Database schemas using Repository Creation Utility, or the prefix that must be used when the deployment tool creates the new schemas. For example, `EDGIGD`
    - **Service Name**: This is the service name of the database service. For example, `IGDEDG.example.com` (`OIM_DB_SERVICENAME`)
    - **Schema Password**: This is the password you used when creating the Oracle Identity Manager schema using RCU or the password you wish to assign to the schemas as they are newly created (`OIM_SCHEMA_PASSWORD`).

    Select **RAC Database**, and provide the following information:

    - **Scan address**: This is the Grid Infrastructure SCAN Address. For example, `IGDDBSCAN.example.com` (`SCAN_ADDRESS`)
    - **Scan Port**: This is the SCAN port. For example, `1521`
    - **ONS Scan Address**: The default value of the Oracle Notification Server (ONS) Scan address used by Gridlink, is the Database scan address.
    - **ONS Port**: This is the port of the Oracle Notification Server (ONS). For example, `6200`

    Click **Next**.

11. Use the Configure SOA screen to enter the listen port for the SOA Managed Servers.

    Click **Next**.

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

    Click **Next**.

13. Use the Set User Names and Passwords screen to set the passwords for the accounts that will be created during deployment. You can set a common password for all of the user accounts listed, or you can set individual passwords for each of the accounts. It is also possible to change some of the default user names.

    To enter a common password for all the accounts to be created, enter the password (*COMMON_IAM_PASWORD*) in the **Enter Common IAM Password** field, and then re-enter the password in the **Confirm Common IAM Password** field.

    If you want to create unique passwords for each account, select **Modify the Username and Password for the user accounts**, and select **Edit** next to the account you wish to modify.

    Click **Next**.

14. Use the Load Balancer screen to provide the following Load Balancer Entry points for the governance domain:

    - **Identity Governance Administration Server**: `igdadmin.example.com`
    - **Identity Internal Call Backs**: `igdinternal.example.com`
    - **Governance**: `prov.example.com`

    Click **Next**.

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

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

    Once the response file creation process is completed, click **Finish** to exit the wizard.

    Note: The Identity and Access Management Deployment Wizard creates a deployment response file in the directory that you specify on the **Summary** screen. It also creates a folder named `responsefilename_data`. For example, `provisioning_data`. This folder contains the `cwallet.sso` file, which has encryption and decryption information. If you move or copy the deployment response file to another location, you must also move or copy the `responsefilename_data` folder containing the `cwallet.sso` file to the same location.

25.4 Creating a Deployment Response File for Oracle Access Manager (OAM) Only Topology

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

1. Perform the steps in Section 25.2, "Starting the Deployment Wizard and Navigating the Common Screens".

2. On the Select IAM Products screen, select **Oracle Access Manager (OAM) Suite and Oracle Mobile Security Suite (OMSS)* Only**.

   Notes: After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection. If you need to make any modification in the previous screens, click **Cancel** and then restart the Oracle Identity and Access Management Deployment Wizard.

3. On the Directory Selection screen, select **Use Existing Directory**. Creating a new directory is not supported for highly available deployments.

   Choose the directory type from the following choices:

   - Oracle Unified Directory
   - Oracle Internet Directory
   - Microsoft Active Directory

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

   After you have chosen your directory type, you have the option of the LCM tool preparing the directory for you. Preparation involves adding object classes to support OAM and seeding the directory with users. If you wish to do this manually, follow the instructions described in Chapter 13, "Preparing The Identity Store".

   Note: IDMLCM prepares the directory for you only if you are performing your deployment using the single `prov_run` command as described in Section 26.3.1, "Running the Deployment Commands Automatically".

   If you are running the deployment commands manually, the IDMLCM will not prepare the ID store for you. You must prepare the ID store manually. You must decide which deployment method you are going to use before selecting this option. If you select this option and then choose to do the deployment manually, the deployment will fail, and the error messages will not identify this as a cause.

   For this example, we will assume you wish the LCM tool to prepare the directory for you.

   Click **Next**.

4. On the Select Topology screen, select **Highly Available**.

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

> **Note:** On a multi-networked host, the host name entered (without the domain) must be same as the result returned from the `hostname` command issued on the machine.
>
> If you have multiple network cards and if you wish to provision using one other than that attached to the default hostname for the duration of provisioning, you must set the hosts hostname to that associated with the value you enter here. This is particularly important on Exalogic Deployments.

For example:

First Instances:

Directory: `ldaphost1.example.com`

Access Management: `oamhost1.example.com`

Web Tier: `ohshost1.example.com`

Second Instances:

Directory: `ldaphost2.example.com`

Access Management: `oamhost2.example.com`

Web Tier: `ohshost2.example.com`

If you are using an existing directory, you will not be asked for the directory host.

If your WEBHOSTs are in a DMZ, select **Install Web Tier in DMZ**. If you select this option, the Oracle Web tier binaries will be installed locally on those hosts. If you deselect it, they will be installed onto shared storage.

If your Directory Hosts are in a dedicated zone confined by a firewall, and if you have created a separate disk share for your Directory executables, then select **Install Directory Into a Dedicated Zone**.

If you wish to use Oracle Access Manager but not use Oracle Mobile Security suite then deselect the **Enable OMSS** box.

> **Note:** It is recommended that, if you wish to use Oracle Mobile Security Suite, create a dedicated domain for it. Therefore, select this option only for the domain where you will run OMSS.
>
> If you are deploying on Exalogic and if you are not using an External OHS, then deselect **Install Directory into a dedicated zone** and **Install WebTier in DMZ**.
>
> If you are deploying on Exalogic and if you are using an External OHS, then deselect **Install Directory into a dedicated zone** but select **Install WebTier in DMZ**.

Click **Next**.

5. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions. For more information about the directories, see Chapter 7, "Preparing Storage for an Enterprise Deployment".

The following are the fields on this screen:

- **Lifecycle Management Store Location**: *LCM_HOME*
- **Mounted on Webhosts**: Select this option if *LCM_HOME* directory needs to be mounted on WEBHOST1 and WEBHOST2 during installation. This is the recommended approach.
- **Software Repository Home**: *REPOS_HOME*
- **Software Installation Location**: *IDM_TOP*
- **Shared Configuration Location**: *SHARED_CONFIG_DIR*
- **Local Configuration Location**: *LOCAL_CONFIG_DIR*

Note: : If you have already run the deployment tool to create a deployment and you wish to run it again to create a second deployment; for example, if you have run the tool for OAM Only and are now running the tool again for OIM Only, the Software Installation Location MUST be different for each installation, whereas the configuration directories can be the same. This is a limitation in this version of the deployment tool.

Click **Next**.

6. Use the Configure Virtual Hosts screen to enter the virtual host names used by each component. For example:

   Access Domain Admin Server: `iadadminvhn.example.com`

   You can also change the listen address of the OAM Managed servers by specifying a virtual host name. Complete this information when the hosts physical hostname is attached to a different network from that which you wish to use. This is most likely going to be the case in Exalogic Deployments. If you are not using a different network, then you should use the physical host name of the servers hosting the OAM Managed Servers.

   Click **Next**.

7. Use the Directory Configuration screen to supply the details of your LDAP directory.

   - First Instance Details

     These are the details of the first LDAPHOST. The tool needs these details to connect to the directory host and configure the LDAP instance.

     – **Host**: This is the host name of one of the LDAP directory instances. For example, `ldaphost1.example.com`

     – **Port**: This is the port that the first instance is using on the server. For example, `1389` (*LDAP_PORT*)

     – **AdminServer Connector Port**: This is the connector port of the Administration Server. This filed is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool.

     – **Instance Home Directory**: This is the absolute path the first directory instance home. This filed is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool.

   - Second Instance Details

These are the details of the second LDAPHOST. The tool needs these details to connect to the directory host and configure the LDAP instance. The second instance will only appear for OUD directories.

Note: If you have more than two directory instances, you must shutdown the remaining instances and create the indexes and ACI's on those instances manually.

For more information, see Section 13.5, "Preparing OID and OUD as the Identity Store".

This configuration should be done only after provisioning has completed.

- **Host**: This is the host name of the second directory instance. For example, `ldaphost2.example.com`
- **Port**: This is the port that the first instance is using on the server. For example, `1389` (*`LDAP_PORT`*)
- **AdminServer Connector Port**: This is the connector port of the Administration Server. This filed is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool.
- **Instance Home Directory**: This is the absolute path the second directory instance home. This filed is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool.

- Directory Details

  These are the details of how applications will connect to the LDAP directory. Applications will not connect to the LDAP instances directly but via the load balancer.

  - **Directory Host**: This is the load balancer entry point for the existing directory. For example, `idstore.example.com`
  - **Directory Port**: This is the port on the load balancer where LDAP requests are sent. For example, `1389` (OUD), `3060` (OID), `389` (AD) (*`LDAP_LBR_PORT`*)
  - **Administrator**: This is the user name of a directory administrator. For example, `cn=oudadmin`
  - **Administrator Password**: This is the password of the directory administrator.
  - **Root CA Certificate for AD**: The location of the active directory certificate. This is applicable only if the directory is Active Directory.

- Container Details

  These are the locations in the directory where Users, Groups and System IDs are stored. System IDs are used to allow products such as, OAM to connect to the LDAP directory without using the administrator account.

  - **Realm DN**: This is the main realm of the directory. For example, `dc=example,dc=com`
  - **Users Groups/Present in the Directory**: Normally, this is left unchecked for a new installation. If you have prepared the installation manually, then select this option.

  - **Users Container**: This is the location within the LDAP directory tree where users are stored.
  - **Groups Container**: This is the location within the directory tree where Groups are stored.
  - **System IDs Container**: This is the location within the directory tree where system users are stored. These are users that allow OAM and OIM to connect to LDAP. They are separated from the main Users container to prevent them being reconciled into OIM.
  - **Users/Groups Present in Directory**: This checkbox is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool. Select this if users or groups are present in your directory.

- Additional Details

  The following are the additional details you must specify, depending on your directory selection:

  - **OUD Replication Port**: This is the replication port of OUD. This filed is displayed if you selected existing directory as OUD, and chose to prepare directory using IDM LCM tool.

- **SSL Enabled**: This checkbox is displayed if you selected your existing directory as Active Directory. For OAM-only topology, this checkbox is unchecked by default, and is editable. For OIM-OAM integrated topology, this checkbox is checked by default, and is not editable.

  If this checkbox is unchecked, the **Directory Port** is set to `389` by default. If this checkbox is checked, the **Directory Port** is replaced by **SSL Port** and is set to `636` by default.

After you specify the required details, click **Next**.

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

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

   Click **Next**.

9. Use the Configure Oracle Access Manager screen to view or modify the ports that will be used by the Oracle Access Manager Managed Servers.

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

   It is also possible to change the Cookie domain, although this will usually refer to the same as the Realm used in LDAP.

   Click **Next**.

10. Use the Configure Oracle Mobile Security Manager screen to view or modify the ports that will be used by Oracle Mobile Security Manager Managed Servers.

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

    Click **Next**.

11. Use the Configure Oracle Mobile Security Access Server screen to view or modify the ports that will be used by Oracle Mobile Security Access Server (MSAS). You can also change the Gateway Instance Id.

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

    Click **Next**.

12. Use the Access Policy Manager screen to review or change the ports that will be used by the Oracle Access Policy Manager Managed Servers.

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

    Click **Next**.

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

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

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

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

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

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

    The following fields are present in this screen:

    - **SYSDBA Username**: This is the name of the SYSDBA account on the database. For example, `sys`
    - **SYSDBA Password**: This is the password for the SYSDBA account.

      SYSDBA credentials are required only if you select **Create Schema Using RCU** option.
    - **Schema Prefix**: This is the prefix that was used when you created Database schemas using Repository Creation Utility, or the prefix that must be used when the deployment tool creates the new schemas. For example, `EDGIAD`
    - **Service Name**: This is the service name of the database service. For example, `IADEDG.example.com` (`OAM_DB_SERVICENAME`)
    - **Schema Password**: This is the password you used when creating the Oracle Identity Manager schema using RCU or the password you wish to assign to the schemas as they are newly created (`OAM_SCHEMA_PASSWORD`).

    Select **RAC Database**, and provide the following information:

    - **Scan address**: This is the Grid Infrastructure SCAN Address. For example, `IADDBSCAN.example.com` (`SCAN_ADDRESS`)
    - **Scan Port**: This is the SCAN port. For example, `1521`

- **ONS Scan Address**: The default value of the Oracle Notification Server (ONS) Scan address used by Gridlink, is the Database scan address.
- **ONS Port**: This is the port of the Oracle Notification Server (ONS). For example, `6200`

Click **Next**.

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

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

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

    If you are using an existing LDAP Directory service, then this screen will also allow you to specify the details of the users and groups you created in the directory in the Preparing an Existing Directory section of this document.

    Click **Next**.

15. Use the Load Balancer screen to provide the Load Balancer Entry points for the Access domain. For example:

    Access Domain Administration Server: `iadadmin.example.com`

    Access Internal Call Backs: `iadinternal.example.com`

    Access SSO: `login.example.com`

    Oracle Mobile Security Access Server: `msas.example.com`

    Click **Next**.

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

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

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

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

25.5 Creating a Deployment Response File for a Fully Integrated Topology

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

1. Perform the steps in Section 25.2, "Starting the Deployment Wizard and Navigating the Common Screens".
2. On the Select IAM Products screen, select **OIM-OAM-OMSS Integrated with Directory***.

   > **Notes:** After you select the components you want to deploy, do not click the **Back** button in the subsequent screens to modify your product selection.
   >
   > If you need to make any modification in the previous screens, click **Cancel** and then restart the Oracle Identity and Access Management Deployment Wizard.

3. On the Directory Selection screen, select **Use Existing Directory**. Creating a new directory is not supported for highly available deployments.

   Choose the directory type from the following choices:

   - Oracle Unified Directory
   - Oracle Internet Directory
   - Microsoft Active Directory

   After you have chosen your directory type, you have the option of the LCM tool preparing the directory for you. It is recommended that you let the tool do it. If you wish to do this manually, follow the instructions described in Chapter 13, "Preparing The Identity Store".

   For this example, we will assume you wish the LCM tool to prepare the directory for you.

   > **Note:** This is supported only if you are using the `prov_run` command to perform the deployment. The `prov_run` command performs the entire deployment automatically. If you are running the deployment manually using the `runIAMDeployment` commands, IDMLCM directory preparation is not supported.

Click **Next**.

4. On the Select Topology screen, select **Highly Available**.

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

   > **Note:** On a multi-networked host, the host name entered (without the domain) must be same as the result returned from the `hostname` command issued on the machine.
   >
   > If you have multiple network cards and if you wish to provision using one other than that attached to the default hostname for the duration of provisioning, you must set the hosts hostname to that associated with the value you enter here. This is particularly important on Exalogic Deployments.

   First Instances:

   - **Directory**: `ldaphost1.example.com`
   - **Identity and Governance**: `oimhost1.example.com`
   - **Access Management**: `oamhost1.example.com`
   - **Web Tier**: `ohshost1.example.com`

   Second Instances:

   - **Directory**: `ldaphost2.example.com`
   - **Identity and Governance**: `oimhost2.example.com`
   - **Access Management**: `oamhost2.example.com`
   - **Web Tier**: `ohshost2.example.com`

   If you are using an existing directory, you will not be asked for the directory host.

   If your WEBHOSTs are in a DMZ, select **Install Web Tier in DMZ**. If you select this option, the Oracle Web tier binaries will be installed locally on those hosts. If you deselect it, they will be installed onto shared storage.

   If your Directory Hosts are in a dedicated zone confined by a firewall, and if you have created a separate disk share for your Directory executables, then select **Install Directory Into a Dedicated Zone**.

   If you wish to use Oracle Access Manager but not use Oracle Mobile Security suite then deselect the **Enable Oracle Mobile Security Suite** box.

   > **Note:** It is recommended that, if you wish to use Oracle Mobile Security Suite, create a dedicated domain for it. Therefore, select this option only for the domain where you will run OMSS.

   If you are deploying on Exalogic and if you are not using an External OHS, then deselect **Install Directory into a dedicated zone** and **Install WebTier in DMZ**.

   If you are deploying on Exalogic and if you are using an External OHS, then deselect **Install Directory into a dedicated zone** but select **Install WebTier in DMZ**.

   Click **Next**.

5. Use the Select Installation and Configuration Locations screen to supply the location of the important directories required for installation and configuration actions. For more information about the directories, see Chapter 7, "Preparing Storage for an Enterprise Deployment".

   The following are the fields on this screen:

   - **Lifecycle Management Store Location**: *LCM_HOME*
   - **Mounted on Webhosts**: Select this option if *LCM_HOME* directory is mounted on WEBHOST1 and WEBHOST2 during installation. This is the recommended approach.
   - **Software Repository Home**: *REPOS_HOME*
   - **Software Installation Location**: *IDM_TOP*
   - **Shared Configuration Location**: *SHARED_CONFIG_DIR*
   - **Local Configuration Location**: *LOCAL_CONFIG_DIR*

   Click **Next**.

6. Use the Configure Virtual Hosts screen to enter the virtual host names used by each component.

   For example:

   Access Domain Admin Server: `iadadminvhn.example.com`

   OAM Server 1: `oamhost1.example.com` (*)

   OAM Server 2: `oamhost2.example.com` (*)

   OAM Policy Manager Server 1: `oamhost1.example.com` (*)

   OAM Policy Manager Server 2: `oamhost2.example.com` (*)

   OMSM Server 1: `oamhost1.example.com` (*)

   OMSM Server 2: `oamhost2.example.com` (*)

   (*) Specify the physical hostname for OAM Managed servers UNLESS you are using a multi networked computer and you wish traffic to use an alternative network. This will be the case with Exalogic.

   Identity Governance Domain Admin Server: `igdadminvhn.example.com`

   SOA Server 1: `oimhost1vhn2.example.com`

   SOA Server 2: `oimhost2vhn2.example.com`

   OIM Server 1: `oimhost1vhn1.example.com`

   OIM Server 2: `oimhost2vhn1.example.com`

   BIP Server 1: `oimhost1vhn3.example.com`

   BIP Server 2: `oimhost2vhn3.example.com`

   Click **Next**.

7. Use the Directory Configuration screen to supply the details of your LDAP directory.

   - First Instance Details

     These are the details of the first LDAPHOST. The tool needs these details to connect to the directory host and configure the LDAP instance.

  - **Host**: This is the host name of one of the LDAP directory instances. For example, `ldaphost1.example.com`
  - **Port**: This is the port that the first instance is using on the server. For example, `1389` (*`LDAP_PORT`*)
  - **AdminServer Connector Port**: This is the connector port for the Administration Server. For example, `4444` (*`LDAP_ADMIN_PORT`*)
  - **Instance Home Directory**: This is the path to the instance home directory. For example, `/u02/private/oracle/config/instances/oud1 (LDAP_ORACLE_INSTANCE)`

- Second Instance Details

  These are the details of the second LDAPHOST. The tool needs these details to connect to the directory host and configure the LDAP instance. The second instance will only appear for OUD directories.

  Note: If you have more than two directory instances, you must shutdown the remaining instances and create the indexes and ACI's on those instances manually.

  For more information, see Section 13.5, "Preparing OID and OUD as the Identity Store".

  This configuration should be done only after provisioning has completed.

  - **Host**: This is the host name of the second directory instance. For example, `ldaphost2.example.com`
  - **Port**: This is the port that the first instance is using on the server. For example, `1389` (*`LDAP_PORT`*)
  - **AdminServer Connector Port**: This is the connector port for the Administration Server. For example, `4444` (*`LDAP_ADMIN_PORT`*).
  - **Instance Home Directory**: This is the path to the instance home directory. For example, `/u02/private/oracle/config/instances/oud2 (LDAP_ORACLE_INSTANCE)`.

- Additional Details
  - **OUD Replication Port**: This is the Oracle Unified Directory replication port. For example, `8989`.

- Directory Details

  These are the details of how applications will connect to the LDAP directory. Applications will not connect to the LDAP instances directly but via the load balancer.

  - **Directory Host**: This is the load balancer entry point for the existing directory. For example, `idstore.example.com`
  - **Directory Port**: This is the port on the load balancer where LDAP requests are sent. For example, `1389` (OUD), `3060` (OID), `389` (AD) (*`LDAP_LBR_PORT`*)
  - **Administrator**: This is the user name of a directory administrator. For example, `cn=oudadmin`

  - **Administrator Password**: This is the password of the directory administrator.
  - **Root CA Certificate for AD**: The location of the active directory certificate. This is applicable only if the directory is Active Directory.

- Container Details

  These are the locations in the directory where Users, Groups and System IDs are stored. System IDs are used to allow products such as OIM and OAM to connect to the LDAP directory without using the administrator account.

  - **Realm DN**: This is the main realm of the directory. For example, `dc=example,dc=com`
  - **Users Groups/Present in the Directory**: Normally, this is left unchecked for a new installation. If you have prepared the installation manually, then select this option.
  - **Users Container**: This is the location within the LDAP directory tree where users are stored.
  - **Groups Container**: This is the location within the directory tree where Groups are stored.
  - **System IDs Container**: This is the location within the directory tree where system users are stored. These are users that allow OAM and OIM to connect to LDAP. They are separated from the main Users container to prevent them being reconciled into OIM.

Click **Next**.

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

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

   Click **Next**.

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

   Set the **Location of the JMS/Tlogs** to the shared storage location where you are placing runtime artifacts. For example:

   RT_HOME`/domains/IAMGovernanceDomain`

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

   Select **Configure Email Server** if you want to identify and configure a mail server so that Oracle Identity Manager can send email notifications. If you wish to configure the Email Server, you must provide the following information:

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

- **Username**: This is username (`EMAIL_USER`) you use to authenticate with the Email server.
- **Password**: This is the password (`EMAIL_PASSWORD`) for the above user.
- **Web Proxy Host**: This is the port of your proxy server if you use one.
- **Web Proxy Port**: This is the host name of your proxy server if you use one.

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

    If you have already installed the schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU), then do not select the **Create Schema Using RCU** check box. In this case, you must provide the required information to connect to the database where the schemas are installed:

    If you have not installed the schemas already, then select **Create Schema Using RCU**. If you choose this option, the LCM Tool creates the schemas as part of the deployment process.

    The following fields are present in this screen:

    - **SYSDBA Username**: This is the name of the SYSDBA account on the database. For example, `sys`
    - **SYSDBA Password**: This is the password for the SYSDBA account.

      SYSDBA credentials are required only if you select **Create Schema Using RCU** option.
    - **Schema Prefix**: This is the prefix that was used when you created Database schemas using Repository Creation Utility, or the prefix that must be used when the deployment tool creates the new schemas. For example, `EDGIGD`
    - **Service Name**: This is the service name of the database service. For example, `IGDEDG.example.com` (`OIM_DB_SERVICENAME`)
    - **Schema Password**: This is the password you used when creating the Oracle Identity Manager schema using RCU or the password you wish to assign to the schemas as they are newly created (`OIM_SCHEMA_PASSWORD`).

    Select **RAC Database**, and provide the following information:

    - **Scan address**: This is the Grid Infrastructure SCAN Address. For example, `IGDDBSCAN.example.com` (`SCAN_ADDRESS`)
    - **Scan Port**: This is the SCAN port. For example, `1521`
    - **ONS Scan Address**: The default value of the Oracle Notification Server (ONS) Scan address used by Gridlink, is the Database scan address.
    - **ONS Port**: This is the port of the Oracle Notification Server (ONS). For example, `6200`

    Click **Next**.

11. Use the Configure SOA screen to enter the listen port for the SOA Managed server.
    - **SOA Host**: This field is purely informational and displays the host on which the product will run.
    - **Port**: Specify the port number to be used by the SOA Server.

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

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

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

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

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

    ```
    .example.com
    ```

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

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

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

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

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

    Change the name of the Gateway Instance Id to `EDGMSAS`. For the rest of the fields, you can use the default values, unless you have similar software running on the same host and you think there might be port conflicts.

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

16. Use the Configure Access Policy Manager screen to review or change the ports that will be used by the Oracle Access Policy Manager Managed Servers.

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

    Click **Next**.

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

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

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

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

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

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

The following fields are present in this screen:

- **SYSDBA Username**: This is the name of the SYSDBA account on the database. For example, `sys`
- **SYSDBA Password**: This is the password for the SYSDBA account.

  SYSDBA credentials are required only if you select **Create Schema Using RCU** option.
- **Schema Prefix**: This is the prefix that was used when you created Database schemas using Repository Creation Utility, or the prefix that must be used when the deployment tool creates the new schemas. For example, `EDGIAD`
- **Service Name**: This is the service name of the database service. For example, `IADEDG.example.com` (`OAM_DB_SERVICENAME`)
- **Schema Password**: This is the password you used when creating the Oracle Identity Manager schema using RCU or the password you wish to assign to the schemas as they are newly created (`OAM_SCHEMA_PASSWORD`).

Select **RAC Database**, and provide the following information:

- **Scan address**: This is the Grid Infrastructure SCAN Address. For example, `IADDBSCAN.example.com` (`SCAN_ADDRESS`)
- **Scan Port**: This is the SCAN port. For example, `1521`
- **ONS Scan Address**: The default value of the Oracle Notification Server (ONS) Scan address used by Gridlink, is the Database scan address.
- **ONS Port**: This is the port of the Oracle Notification Server (ONS). For example, `6200`

Click **Next**.

18. Use the Set User Names and Passwords screen to set the passwords for the accounts that will be created during deployment. You can set a common password for all of the user accounts listed, or you can set individual passwords for each of the accounts. It is also possible to change some of the default user names.

    To enter a common password for all the accounts to be created, enter the password in the **Enter Common IAM Password** (*`COMMON_IAM_PASWORD`*) field, and then re-enter the password in the **Confirm Common IAM Password** field.

    If you want to create unique passwords for each account, select **Modify the Username and Password for the user accounts**, and select **Edit** next to the account you wish to modify.

    If you are using an Existing LDAP directory, then this screen will also allow you to specify the details of the users and groups you created in the directory in Chapter 13, "Preparing The Identity Store".

    Click **Next**.

19. Use the Load Balancer screen to provide the Load Balancer Entry points for both Access domain and Governance domain. For example:

    Access Domain Administration Server: `iadadmin.example.com`

    Identity Governance Administration Server: `igdadmin.example.com`

Identity Internal Call Backs: `igdinternal.example.com`

Access Internal Call Backs: `iadinternal.example.com`

Access SSO: `login.example.com`

Governance: `prov.example.com`

Oracle Mobile Security Access Server: `msas.example.com`

Click **Next**.

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

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

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

26

Deploying Identity and Access Management

This chapter describes how to deploy Identity and Access Management.

It contains the following sections:

26.1 Introduction to the Deployment Process

This section introduces the deployment process. This section includes the following topics:

26.1.1 Deployment Stages

There are eight stages to Deployment. These stages are:

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

- Associates Access Manager with Oracle Unified Directory
- Configure Oracle Identity Manager

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

Each stage must be completed on all hosts in a specific order, as described in the next section. Each stage must be completed on each host in the topology before the next stage can begin. Failure of a stage will necessitate a cleanup and restart.

26.1.2 Processing Order

Deployment processes the hosts in the following order:

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

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

Consolidated Topology Processing Order

1. IAMHOST1
2. IAMHOST2

Distributed Topology Processing Order

1. OIMHOST1
2. OIMHOST2
3. OAMHOST1
4. OAMHOST2
5. WEBHOST1
6. WEBHOST2

Note: For Exalogic Physical use the Consolidated Topology Steps.

For Exalogic Virtual use the Distributed Topology Steps.

26.2 Prerequisites for Deployment on Exalogic

Before you start the deployment on Exalogic, you must complete the following prerequisites:

1. Install and configure Oracle Traffic Director (OTD).

   For information about installing Oracle Traffic Director, see Section 11.2.2, "Installing Oracle Traffic Director".

   For information about configuring Oracle Traffic Director, see Section 14.2, "Configuring Oracle Traffic Director".

2. Use a dummy port number for OTD. For more information, see the Note in Section 14.2.3, "Creating a Configuration".

3. Ensure that you create a dummy entry in the hosts file.

   In Exalogic, internal requests are load balanced by OTD. When performing a deployment using Life Cycle Management Tool, the load balancer entry points, *iadinternal.example.com*:7777 and *igdinternal.example.com*:7777 are managed by OTD. When you set OTD to use a dummy port number, those URLs become inaccessible. This does not cause an issue for Oracle Identity Manager, but Oracle MSAS configuration will fail, as it requires access to the WebLogic `wls_msm` Managed Servers during configuration.

   To workaround this issue, you must change the entry in the `/etc/hosts` file for `iadinternal` to point to the OTD host. This makes it look like the *iadinternal.example.com* exists and is working. For example:

   On WEBHOST1, the `/etc/hosts` file looks like:

   ```
   10.10.10.1 webhost1.example.com
   192.168.50.1 iadinternal.example.com
   ```

   Change this to:

   ```
   10.10.10.1 webhost1.example.com
   10.10.10.1 iadinternal.example.com
   ```

   This makes the MSAS configuration access the OHS server on OTD host1 which will then be able to pass on requests to the `wls_msm` Managed Servers.

   You must make these changes on both the WEBHOSTS. Ensure that you assign the value to the local WEBHOST. After the deployment is complete, remove the dummy entries.

26.3 Deployment Procedure

In previous releases of the configuration Wizard, each phase of the process needed to be initiated manually on each host in the topology. This is still a supported method. However, in this release, you can provision the entire environment using two simple commands. For completeness, both options are shown below:

- Section 26.3.1, "Running the Deployment Commands Automatically"
- Section 26.3.2, "Running the Deployment Commands Manually"

- Section 26.3.3, "Creating Backups"

26.3.1 Running the Deployment Commands Automatically

Choose a host to initiate provisioning from. This should be one of the application tier hosts, this will be known henceforth as the master host. The master host is the node where you are running the deployment.

This process sets up SSH equivalence on each node. This is required for the duration of the deployment. It can be disabled later if desired.

26.3.1.1 Preparing the Hosts for Automated Deployment

From the master node, execute the command `prov_setup_ssh.sh`, which is located in the following directory:

IDMLCM_HOME`/provisioning/bin`

Run the following command:

```
./prov_setup_ssh.sh -responseFile <Absolute_Path_to_the_deployment_file>
```

For example:

```
cd IDMLCM_HOME/provisioning/bin

./prov_setup_ssh.sh -responseFile
/u01/lcm/tools/idmlcm/provisioning/bin/provisioning.rsp
```

When asked whether or not you wish to enable SSH, enter **Yes** and press **Return**.

The script now connects to each of the hosts in your topology. When it does, it may prompt you to verify the authenticity of the host by showing you the hosts RSA fingerprint and asking if you wish to continue connecting. Enter **Yes** and press **Return**.

It prompts you for the password of the account you are using on the remote host. It repeats this process for each host in the topology. Keep entering the passwords as prompted until the script finishes. At that time, it can remotely execute commands on those hosts without the need for a password. This is ssh equivalence.

After the deployment is complete, ssh equivalence is removed.

26.3.1.2 Deploying Identity and Access Management Automatically

Now that you have set up ssh on the hosts, start the deployment. You can start the deployment by running `prov_run.sh` command from the same directory. For example:

```
set JAVA_HOME to JAVA_HOME

cd IDMLCM_HOME/provisioning/bin

./prov_run.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
```

26.3.2 Running the Deployment Commands Manually

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

IDMLCM_HOME`/provisioning/bin`

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

Notes:

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

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

- Set JAVA_HOME to: *REPOS_HOME*/jdk

The commands you must run are:

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

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

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

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

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

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

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

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

26.3.3 Creating Backups

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

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

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

26.4 Check List

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

Virtual

Deployment Stage	Host	Complete
Preverify	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Install	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Preconfigure	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Configure	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Configure Secondary	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Post Configure	OIMHOST1	
	OIMHOST2	

Deployment Stage	Host	Complete
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Startup	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	
Validate	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	

26.5 Deploying Identity and Access Management Without a Common LCM_HOME

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

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

1. Create a local version of the *LCM_HOME* directory, including the software repository.
2. Copy the Deployment Response File, *responsefilename*_data folder, and Summary created in Chapter 25, "Creating a Deployment Response File" to the same location on each of the hosts.
3. The deployment tool relies on the contents of the directories located under LCM_HOME/provisioning to determine what stages have run successfully. Therefore, after every command, copy the contents of this directory to every node before executing any runIAMDeployment.sh commands.
4. Before running preconfigure on OIMHOST1, copy *LCM_HOME*/keystores from OAMHOST1 to OIMHOST1.
5. If *LCM_HOME* is not mounted on WEBHOST1 and WEBHOST2 (or OHSHOST1/OHSHOST2 in a topology with external Oracle HTTP Servers), before execution of the postconfigure phase on WEBHOST1, copy *LCM_HOME*/keystores/webgate_artifacts from OAMHOST1 to WEBHOST1 and WEBHOST2

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

27

Performing Post-Deployment Configuration

This chapter describes tasks you must perform after deployment using LCM tools.

Once the deployment using LCM tools is complete, you can perform the basic functions in the system. Connect to each Administration Server and ensure that all of the Managed Servers are up and running. After you verify that the servers are up and running, perform the following post-deployment tasks specific to various components to make the system fully ready:

- Post Deployment Steps for Exalogic Implementations
- Post-Deployment Steps for Oracle Unified Directory
- Post-Deployment Steps for Oracle Identity Manager
- Post Deployment Steps for Oracle BI Publisher
- Post Deployment Steps for Oracle Mobile Security Suite
- Post-Deployment Steps for Access Manager
- Adding a Load Balancer Certificate to Trust Stores
- Creating a Redundant Middleware Home
- Restarting All Components

27.1 Post Deployment Steps for Exalogic Implementations

This section describes post-deployment steps for Exalogic Implementations.

This section contains the following topics:

- Section 27.1.1, "Enabling Oracle Traffic Director as Web Server"
- Section 27.1.2, "Reverting Host Name changes"
- Section 27.1.3, "Enabling WebLogic Domain Exalogic Optimization"
- Section 27.1.4, "Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager, SOA, and BI"
- Section 27.1.5, "Forcing Oracle Identity Manager to use the Correct Multicast Address"
- Section 27.1.6, "Enabling Oracle Access Manager Persistence Optimizations"
- Section 27.1.7, "Configuring Oracle Identity Manager Servers to Listen on EoIB"
- Section 27.1.8, "Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment"

27.1.1 Enabling Oracle Traffic Director as Web Server

This Section describes how to enable OTD as a web server. If you are using external Oracle HTTP servers, skip this section, as the Oracle HTTP Servers are providing the web server functionality.

This section includes the following topics:

- Section 27.1.1.1, "Stopping the OHS Servers"
- Section 27.1.1.2, "Stopping the OHS Servers from Starting and Stopping Automatically"
- Section 27.1.1.3, "De-registering OHS servers from Domain"
- Section 27.1.1.4, "Resetting the Oracle Traffic Director Listen Port"

27.1.1.1 Stopping the OHS Servers

Stop the Oracle HTTP servers that the provisioning wizard created by executing the `opmnctl` command, which is located in the directory *`OHS_ORACLE_INSTANCE`*`/bin`, as follows:

```
opmnctl stopall
```

Run this command on both `WEBHOST1` and `WEBHOST2`.

27.1.1.2 Stopping the OHS Servers from Starting and Stopping Automatically

To stop the OHS servers starting and stopping automatically, proceed as follows:

1. Edit the file `serverInstancesInfo.txt` which is located at *`SHARED_CONFIG_DIR`*`/scripts`.
2. Comment out the following lines by placing a `#` at the beginning of the line:

   ```
   webhost1 OHS /u02/private/oracle/config/instances/ohs1

   webhost2 OHS /u02/private/oracle/config/instances/ohs2
   ```

3. Repeat on each `WEBHOST`.

27.1.1.3 De-registering OHS servers from Domain

IDMLCM registers the Oracle HTTP Servers with the Access Domain. As you are no longer using OHS, you need to de-register the instances to prevent log files getting filled unnecessarily. You can do this by running the following command:

`OHS_ORACLE_INSTANCE``/bin/opmnctl unregisterinstance`

Enter the WebLogic Administration password when prompted.

27.1.1.4 Resetting the Oracle Traffic Director Listen Port

Now that provisioning is complete and the Oracle HTTP server is disabled, the OTD configuration must be updated with the OHS Listen Port. To do this, complete the following steps:

1. Login to the OTD administration server using the URL:

   ```
   https://OTDADMINVHN:8800
   ```

2. Click **Configurations**, which is at the upper left corner of the page.

   A list of the available configurations is displayed.

3. Select the configuration which you want to amend. For example, **sso.mycompany.com**.
4. Expand **Listeners** in the navigation pane.
5. Click **http-listener-1**.
6. Set the port to *WEB_HTTP_PORT*. For example, 7777.
7. Click **Save**.
8. Click **Deploy Changes**.

27.1.2 Reverting Host Name changes

Before starting a deployment on Exalogic using LCM you created a dummy entry in the /etc/hosts file for the virtual host iadinternal.example.com. Now that the deployment is complete, this dummy entry needs to be replaced with the real entry. This change should be made on both the WEBHOSTs.

For example, on WEBHOST1 the /etc/hosts file looks like:

```
10.10.10.1 webhost1.example.com
10.10.10.1 iadinternal.example.com
```

Change this back to:

```
10.10.10.1 webhost1.example.com
192.168.50.1 iadinternal.example.com
```

By making this change, MSAS configuration will access the web server on OTD host1 which will then be able to pass on requests to the wls_msm managed servers. Ensure that you make this change on both WEBHOSTs by assigning the value to the local web host.

After deployment, these dummy entries should be removed.

27.1.3 Enabling WebLogic Domain Exalogic Optimization

Enable WebLogic domain Exalogic optimizations by following the instructions described in Section 15.4.14.1, "Enabling WebLogic Domain Exalogic Optimization".

27.1.4 Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager, SOA, and BI

You can enable session replication enhancements for Managed Servers in a WebLogic cluster to which you deploy a Web application at a later time.

For information about enabling session replication enhancements for OIM and SOA, see Section 19.20.2, "Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager and SOA".

For information about enabling session replication enhancements for Oracle BI Publisher, see Section 20.6, "Enabling Cluster-Level Session Replication Enhancements for Oracle BI Publisher".

27.1.5 Forcing Oracle Identity Manager to use the Correct Multicast Address

Oracle Identity Manager uses multicast for certain functions. By default, the managed servers communicate using the multi cast address assigned to the primary host name. If you wish multicast to use a different network, for example, of the internal network,

complete the steps described in Section 19.21, "Forcing OIM to use Correct Multicast Address".

27.1.6 Enabling Oracle Access Manager Persistence Optimizations

You can speed up OAM persistence by enabling OAM Exalogic optimizations by adding a new parameter to the server start options for each OAM managed server.

For more information about enabling OPMS optimizations, see Section 17.7.1, "Enabling OAM Persistence Optimizations".

27.1.7 Configuring Oracle Identity Manager Servers to Listen on EoIB

This task is only required if the Oracle Identity Manager servers need to be accessed directly from outside the Exalogic machine. This is the case when external Oracle HTTP Servers are part of the configuration. In such case, you must create a new network channel.

For more information, see Section 19.20.1, "Configuring Oracle Identity Manager Servers to Listen on EoIB".

27.1.8 Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

This section describes how to configure single sign-on (SSO) for administration consoles in an Identity and Access Management Enterprise deployment.

This section includes the following topic:

- Section 27.1.8.1, "Installing and Configuring WebGate for OTD"

27.1.8.1 Installing and Configuring WebGate for OTD

Install and configure WebGate for Oracle Traffic Director. For more information, see Section 22.5, "Installing and Configuring WebGate for Oracle Traffic Director 11g".

27.2 Post-Deployment Steps for Oracle Unified Directory

Perform the following steps for Oracle Unified Directory:

- Section 27.2.1, "Updating Oracle Unified Directory ACIs for LDAP Synchronization"
- Section 27.2.2, "Granting OUD changelog Access"
- Section 27.2.3, "Creating OUD Indexes"

27.2.1 Updating Oracle Unified Directory ACIs for LDAP Synchronization

When LDAP synchronization is enabled, Oracle Unified Directory operations may fail. As a workaround, you must update ACIs on both instances of Oracle Unified Directory.

For more information, see Section 13.5.4, "Updating Oracle Unified Directory ACIs for LDAP Synchronization".

27.2.2 Granting OUD changelog Access

If you had selected Prepare Directory using IDMLCM option during the deployment, you must grant access to the `changelog`. as part of the post-deployment task. For more information, see Section 13.5.3, "Granting OUD changelog Access".

27.2.3 Creating OUD Indexes

Create Oracle Unified Directory indexes as described in Section 13.5.5, "Creating OUD Indexes".

27.3 Post-Deployment Steps for Oracle Identity Manager

Perform the following post-deployment steps.

- Section 27.3.1, "Configuring Oracle Identity Manager to use a Database Persistence Store"
- Section 27.3.2, "Modifying Oracle Identity Manager Properties to Support Active Directory"
- Section 27.3.3, "Setting Memory Parameters"
- Section 27.3.4, "Configuring Server Migration"
- Section 27.3.5, "Updating OIM LDAP Reconciliation Jobs"

27.3.1 Configuring Oracle Identity Manager to use a Database Persistence Store

This task is optional. This section describes how to move the Persistent stores to the database. Moving the persistent stores to the database simplifies Disaster Recovery Setup allowing for JMS messages to be included in the database rather than on the file system.

For more information, see Section 19.19, "Using JDBC Persistent Stores for TLOGs and JMS".

27.3.2 Modifying Oracle Identity Manager Properties to Support Active Directory

If your Identity Store is in Active Directory, modify the Oracle Identity Manager properties as described in Section 19.4, "Modifying the Oracle Identity Manager Properties to Support Active Directory".

27.3.3 Setting Memory Parameters

You start the Administration Server using WLST and connecting to the Node Manager. The first start of the Administration Server with Node Manager requires that you change the default username and password that the Configuration Wizard sets for the Node Manager. This is already performed by the IDMLCM provisioning tool, where the Node Manager admin user password is being set to the *`common IDM password`* value provided during response file creation.

For information on updating the Node Manager credentials, see Section 15.4.5.2, "Updating the Node Manager Credentials".

You must set the memory parameters in the `setDomainEnv.sh` file and restart the Administration Server. For more information, see Section 15.4.3, "Setting IAMAccessDomain Memory Parameters".

27.3.4 Configuring Server Migration

Server Migration is required if one of your OIM hosts goes down partway through a transaction. By configuring server migration, you can ensure that any inflight JMS transactions are processed.

For information about setting up server migration, see Chapter 21, "Configuring Server Migration for an Enterprise Deployment".

27.3.5 Updating OIM LDAP Reconciliation Jobs

As a post-deployment task, update the OIM LDAP reconciliation jobs. For more information, see Section 19.15, "Updating OIM LDAP Reconciliation Jobs".

27.4 Post Deployment Steps for Oracle BI Publisher

This section describes the post-deployment tasks for Oracle BI Publisher.

This section contains the following topics:

- Section 27.4.1, "Configuring Oracle BI Publisher to use a Database Persistence Store"

27.4.1 Configuring Oracle BI Publisher to use a Database Persistence Store

This task is optional.

This section describes how to move the Persistent stores to the database. Moving the persistent stores to the database simplifies Disaster Recovery Setup allowing for JMS messages to be included in the database rather than on the file system. For more information, see Section 15.4.10, "Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment".

27.5 Post Deployment Steps for Oracle Mobile Security Suite

This section describes the post-deployment tasks for Oracle Mobile Security Suite.

This section contains the following topics:

- Section 27.5.1, "Creating OMSS Helpdesk User and Roles"

27.5.1 Creating OMSS Helpdesk User and Roles

Once you have integrated OAM and OIM, create a user for Oracle Mobile Security Suite. For more information, see Section 19.13.5, "Creating OMSS Helpdesk User and Roles".

27.6 Post-Deployment Steps for Access Manager

This section contains the following topics

- Section 27.6.1, "Updating WebGate Agents"
- Section 27.6.2, "Adding Missing Policies to OAM"
- Section 27.6.3, "Updating the ESSO IDS Repository"

27.6.1 Updating WebGate Agents

After deployment, update existing WebGate Agents. For more information, see Section 17.2.4, "Updating WebGate Agents".

27.6.2 Adding Missing Policies to OAM

If you are using Oracle Mobile Security Suite (OMSS), you must add the missing policies to OAM as described in Section 17.2.6, "Adding Missing Policies to OAM".

27.6.3 Updating the ESSO IDS Repository

The ESSO Identity Store Repository is created by default as ssl enabled. If the LDAP connection is not SSL enabled, update the IDS repository to uncheck the ssl flag by completing the steps described in Section 17.6, "Updating the ESSO IDS Repository".

27.7 Adding a Load Balancer Certificate to Trust Stores

Some IAM Products require that the SSL certificate used by the load balancer be added to the trusted certificates in the JDK used by OPAM. For more information about adding the certificates, see Section 15.4.13, "Adding a Load Balancer Certificate to JDK Trust Stores".

27.8 Creating a Redundant Middleware Home

If you wish to create a redundant Middleware Home to protect from binary corruptions, you can do so by following the steps in described in Appendix A, "Creating a Redundant Middleware Home".

27.9 Restarting All Components

Restart all components, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

28

Cleaning up an Environment Before Rerunning IAM Deployment

This chapter describes how to clean up an environment before rerunning Identity and Access Deployment.

This chapter contains the following section:

- Section 28.1, "Cleaning up an Environment"

28.1 Cleaning up an Environment

When you provision Oracle Identity and Access Management using the `runIAMDeployment.sh` command, you must complete each stage in the topology before beginning the next stage, in a specified order. If a stage fails, you must clean up and start over.

> **Note:** The cleanup command provided as part of the LCM tool should not be used for the cleanup of a deployment. The cleanup tool does not support EDG deployments. Cleanup is a manual process and is described in this chapter.

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

1. On each host, stop or kill the Identity and Access Management processes. The simplest way to do this is to restart the host. If this is not possible, manually clean up the processes following your Operating System documentation.
2. On each host, remove the following directories:
   - *LOCAL_CONFIG_DIR*`/domains`
   - *LOCAL_CONFIG_DIR*`/instances/ohs*`
   - *LOCAL_CONFIG_DIR*`/instances/EDGMSAS`

   > **Note:** Exclude this step for an Oracle Traffic Director installation.

3. On each WEBHOST, remove the following directories:
   - *WEB_MW_HOME*`/ohs`
   - *WEB_MW_HOME*`/webgate`

- *WEB_MW_HOME*/omsas

Note: Do not remove any directories belonging to your OTD installation, if you have one.

4. Remove the contents of the following directories on either OAMHOST1 or OIMHOST1:
   - On OAMHOST1, remove:

     IAD_MW_HOME

     SHARED_CONFIG_DIR
   - On OIMHOST1, remove:

     IGD_MW_HOME

     SHARED_CONFIG_DIR

Note: Do not remove the directory *DIR_MW_HOME*.

5. Remove the contents of the following LCM directories:
   - *LCM_HOME*/provisioning
   - *LCM_HOME*/patch
   - *LCM_HOME*/lcmconfig
   - *RT_HOME*

Note: These directories are on shared storage and only needs to be removed from one host

6. Remove all of the directories that were created by the IDMLCM tool during the Identity and Access Management deployment.
7. Using the Repository Creation Utility, drop all schemas created in Section 10.7, "Loading the Identity and Access Management Schemas in the Oracle RAC Database Using RCU."

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

Part V

Managing an Enterprise Deployment

This part includes chapters with information about managing your enterprise deployment.

Part I contains the following chapters:

- Chapter 29, "Scaling Enterprise Deployments"
- Chapter 31, "Managing the Topology for an Enterprise Deployment"

29

Scaling Enterprise Deployments

The reference enterprise topology discussed in this guide is highly scalable. It can be scaled up and or scaled out. This chapter explains how to do so.

To scale up the topology, you add a new component instance to a node already running one or more component instances. To scale out the topology, you add new component instances to new nodes.

This chapter contains the following topics:

29.1 Scaling the Topology

The Oracle Identity and Access Management topology described in the guide has three tiers: the Directory Tier, Application Tier and Web Tier. The components in all three tiers of the Oracle Identity and Access Management topology described in this guide can be scaled up or scaled out.

In this release, the Identity and Access Management Deployment tool cannot be used to scale out or scale up components. Scaling up or out is a manual process, as described in this chapter.

You scale up a topology by adding a new server instance to a node that already has one or more server instances running. You scale out a topology by adding new components to new nodes.

29.2 Scaling the LDAP Directory

This section describes how to scale an LDAP directory.

This section contains the following topics:

29.2.1 Mounting the Middleware Home when Scaling Out

Oracle Binaries are shared among the LDAP hosts. When scaling out, you must mount the shared binary directory onto the new host.To do this, perform the steps in Section 9.11, "Mounting Shared Storage onto the Host."

29.2.2 Scaling Oracle Unified Directory

The binaries for Oracle Unified Directory are located in *IDM_TOP*, which is shared among the LDAPHOSTs. When scaling out Oracle Unified Directory to a new host, ensure that this directory is mounted to the new host. See Section 9.11, "Mounting Shared Storage onto the Host."

The directory tier has two Oracle Unified Directory nodes, LDAPHOST1 and LDAPHOST2, each running an Oracle Unified Directory instance. The Oracle Unified Directory binaries on either node can be used for creating the new Oracle Unified Directory instance.

Proceed as follows:

1. Assemble information, as listed in Section 29.2.2.1, "Assembling Information for Scaling Oracle Unified Directory."
2. If scaling out, mount the shared storage onto the new LDAPHOST.
3. Follow the steps in Section 29.2.2.2, "Configuring an Additional Oracle Unified Directory Instance."
4. Follow the steps in Section 29.2.2.3, "Validating the New Oracle Unified Directory Instance."
5. Follow the steps in Section 29.2.2.4, "Adding the New Oracle Unified Directory Instance to the Load Balancers."
6. Reconfigure the load balancer with the host and port information of the new Oracle Unified Directory instance, as described in Section 29.4.5, "Reconfiguring the Load Balancer."

29.2.2.1 Assembling Information for Scaling Oracle Unified Directory

Assemble the following information before scaling Oracle Unified Directory.

Description	Variable	Documented Value	Customer Value
New Oracle Unified Directory Host Name	*LDAP_HOST*	LDAPHOST3.example.com	
Oracle Unified Directory Listen Port	*LDAP_PORT*	1389	
Oracle Unified Directory SSL Port	*LDAP_SSL_PORT*	1636	
Oracle Unified Directory Administration Port	*LDAP_ADMIN_PORT*	4444	
Oracle Unified Directory Replication Port	*LDAP_REPLIC_PORT*	8989	
Oracle Instance Location	*LDAP_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oud*n*	
Oracle Unified Directory Existing Instance/Component Name	oud*n*	oud1	
Newly Created Instance/Component Name	oud*n*	oud3	

Description	Variable	Documented Value	Customer Value
Oracle Unified Directory Administrator Password	*COMMON_IDM_PASSWORD*		
Common Password	*COMMON_IDM_PASSWORD*		

29.2.2.2 Configuring an Additional Oracle Unified Directory Instance

If you are scaling out to another machine, you can use ports 1389 (*LDAP_PORT*), 1636 *(LDAP_SSL_PORT*), 4444 (*LDAP_ADMIN_PORT*), and 8989 (*LDAP_REPLIC_PORT*). If you are scaling up, those ports are already in use and you must choose unique ports. Ensure that the ports you plan to use are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

```
netstat -an | grep "1389"
```

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

Remove the entries for the ports you freed from the `/etc/services` file and restart the services or restart the computer.

Set the environment variable `JAVA_HOME`

Set the environment variable `INSTANCE_NAME` to a new instance value, such as: `../../../../u02/private/oracle/config/instances/oud3`

Note the tool creates the instance home relative to the *OUD_ORACLE_HOME*, so you must include previous directories to get the instance created in *LDAP_ORACLE_INSTANCE*.

Change Directory to *OUD_ORACLE_HOME*

Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

1. On the Welcome screen, click **Next**.
2. On the Server Settings screen, enter:
   - **Host Name**: The name of the host where Oracle Unified Directory is running, for example: LDAPHOST3
   - **LDAP Listener Port**: 1389 (*LDAP_PORT*) if scaling out, unique port if scaling up.
   - **Administration Connector Port**: 4444 (*LDAP_ADMIN_PORT*)
   - LDAP Secure Access
     - Click **Configure**
     - Select **SSL Access**
     - **Enable SSL on Port**: 1636 *(LDAP_SSL_PORT*)
     - **Certificate**: Generate Self Signed Certificate OR provide details of your own certificate.
     - Click **OK**
   - **Root User DN**: Enter an administrative user for example `cn=oudadmin`

- **Password**: Enter the password you want to assign to the ouadmin user. Using the *COMMON_IDM_PASSWORD* is recommended.
- **Password (Confirm)**: Repeat the password.
- Click **Next**.

3. On the Topology Options screen, enter
   - **This server will be part of a replication topology**
   - **Replication Port:** (*LDAP_REPLIC_PORT*) 8989
   - Select **Configure As Secure,** if you want replication traffic to be encrypted.
   - **There is already a server in the topology**: Selected.

     Enter the following:

     – **Host Name**: The name of the Oracle Unified Directory server host for this instance, for example: LDAPHOST1.example.com

     – **Administrator Connector Port**: 4444 (*LDAP_ADMIN_PORT*)

     – **Admin User**: Name of the Oracle Unified Directory administrative user on LDAPHOST1, for example: `cn=oudadmin`

     – **Admin Password**: Administrator password. Using the *COMMON_IDM_PASSWORD* is recommended.

     Click **Next**.

     If you see a certificate Not Trusted Dialogue, it is because you are using self signed certificates. Click **Accept Permanently.**

   Click **Next**.
4. On The Create Global Administrator Screen Enter:
   - **Global Administrator ID:** The name of an account you want to use for managing Oracle Unified Directory replication, for example: `oudmanager`
   - **Global Administrator Password** / **Confirmation**: Enter a password for this account. Using the *COMMON_IDM_PASSWORD* is recommended.

   Click **Next**.
5. On the Data Replication Screen. select `dc=example,dc=com` and click **Next**.
6. On the Oracle Components Integration screen, click **Next**.
7. On the Runtime Options Screen Click Next.
8. On the Review Screen, check that the information displayed is correct and click **Finish**.
9. On the Finished screen, click **Close**.

29.2.2.3 Validating the New Oracle Unified Directory Instance

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

```
LDAP_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAPHOST3.example.com -p 1389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl
```

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

29.2.2.4 Adding the New Oracle Unified Directory Instance to the Load Balancers

Add the new Oracle Unified Directory instance to the existing server pool defined on the load balancer for distributing requests across the instances.

29.2.3 Scaling Oracle Internet Directory

This section describes how to scale Oracle Internet Directory.

This section contains the following topics:

- Section 29.2.3.1, "Configuring Oracle Internet Directory on LDAPHOST3"
- Section 29.2.3.2, "Validating the installation of OID on LDAPHOST3"

29.2.3.1 Configuring Oracle Internet Directory on LDAPHOST3

To configure Oracle Internet Directory on LDAPHOST3:

1. Ensure that ports 3060 and 3061 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   ```
   netstat -an | grep "3060"
   netstat -an | grep "3061"
   ```

   If the ports are in use (the command returns output identifying either port), you must free the port, or choose a different one.

2. Mount the `SW_ROOT` file system onto the new LDAPHOST (this is the file system which contains the *DIR_MW_HOME*).

3. Copy the `staticports.ini` file from the following directory to a temporary directory on the installation media:

   REPOS_HOME`/installers/idm/Disk1/stage/Response`

4. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports 3060 and 3061, as follows, uncomment the entries in the file corresponding to the entries below and set the values accordingly.

Table 29–1 Oracle Internet Directory Ports

Entry	Value
Oracle Internet Directory Port Number	3060
Oracle Internet Directory (SSL) Port Number	3061

5. Start the Oracle Identity Management 11g Configuration Assistant by running:

   DIR_MW_HOME`/oid/bin/config.sh`

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

7. On the Select Domain screen, select **Configure without a Domain**, and click **Next**.

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

   - **Oracle Instance Location**: *LOCAL_CONFIG_DIR*`/instances/oid2`
   - **Oracle Instance Name**: `oid3`

   Click **Next**.

9. On the Specify Security Updates screen, choose whether to receive security updates from Oracle support, and click **Next**.
10. On the Configure Components screen, select **Oracle Internet Directory**, deselect all the other components, and click **Next**.
11. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
    - **Connect String**: `igddb-scan.example.com:1521:igddb1^ igddb-scan.example.com:1521:igdb2@igdedg.example.com`
    - **User Name**: `ODS`
    - **Password**: Enter the password for the OID schema created by RCU, and click **Next**.

    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 reuses the same schema.

    Click **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 LDAPHOST1, LDAPHOST2 and LDAPHOST3 is synchronized.

    Click **OK** to continue.
12. On the Specify OID Admin Password screen, specify the Oracle Internet Directory administration password that you specified when creating the first OID instance.

    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 Linux and UNIX systems, a dialog box may appear, that prompts you to run the `oracleRoot.sh` script. Run the `oracleRoot.sh` script, as the root user. When prompted:

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

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

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

29.2.3.2 Validating the installation of OID on LDAPHOST3

To validate the installation of the Oracle Internet Directory instance on LDAPHOST3, issue these commands:

```
export ORACLE_HOME=OID_ORACLE_HOME
ORACLE_HOME/bin/ldapbind -h ldaphost2.example.com -p 3060 -D "cn=orcladmin" -q
ORACLE_HOME/bin/ldapbind -h ldapdhost2.example.com -p 3061 -D "cn=orcladmin" -q -U
1
```

You will be prompted for your administrator password.

> **Note:** You must invoke `ldapbind` from the OID Oracle Home. Many LINUX systems come with an `openldap` version of `ldapbind`, which is incompatible with Oracle Internet Directory.

29.3 Scaling Identity and Access Management Applications

The Application Tier has two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Access Management Access Manager, and two nodes (OIMHOST1 and OIMHOST2) running Managed Servers for Oracle Identity Manager. Optionally, the Application Tier might have two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Adaptive Access Manager.

This section contains the following topics:

- Section 29.3.1, "Gathering Information."
- Section 29.3.2, "Mounting Middleware Home and Creating a New Machine when Scaling Out."
- Section 29.3.3, "Creating a New Node Manager when Scaling Out."
- Section 29.3.4, "Running Pack/Unpack."
- Section 29.3.5, "Performing Application-Specific Steps."
- Section 29.3.6, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files."

29.3.1 Gathering Information

Use the following tables to assemble the values you need.

29.3.1.1 Assembling Information for Scaling Access Manager

Assemble the following information before scaling Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	`NEWHOSTn`		
Existing Access Manager server		`WLS_OAM1`	
New Access Manager server name	`WLS_OAMn`	`WLS_OAM3`	
Server Listen Port	*`OAM_PORT`*	14100	
WebLogic Administration Host	*`WLS_ADMIN_HOST`*	IADADMINVHN.example.com	

Description	Variable	Documented Value	Customer Value
WebLogic Administration Port	*IAD_WLS_PORT*	7001	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

29.3.1.2 Assembling Information for Scaling Oracle Identity Manager

Description	Variable	Documented Value	Customer Value
Host name	NEWHOST*n*		
SOA virtual server name		SOAHOST*x*VHN	
Oracle Identity Manager virtual server name		OIMHOST*x*VHN	
Existing SOA managed server to clone	WLS_SOA*n*	WLS_SOA1	
Existing Oracle Identity Manager managed server to clone	WLS_OIM*n*	WLS_OIM1	
New SOA managed server name	WLS_SOA*n*	WLS_SOA3	
New Oracle Identity Manager managed server name	WLS_OIM*n*	WLS_OIM3	
Numeric extension for new JMS servers	*n*	3	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IGDADMINVHN.example.com	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7101	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

29.3.1.3 Assembling Information for Scaling Oracle Adaptive Access Manager

Assemble the following information before scaling Oracle Adaptive Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	*NEWHOSTn*		
Existing OAAM server		WLS_OAAM1	
New OAAM server name	*WLS_OAAMn*	WLS_OAAM3	
Server Listen Address			
OAAM Managed Server Port	*OAAM_PORT*	14300	
OAAM Administration Managed Server Port	*OAAM_ADMIN_PORT*	14200	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IDADMINVHN.example.com[1]	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7001	
WebLogic Administration User		weblogic_idm	

Description	Variable	Documented Value	Customer Value
WebLogic Administration Password			

[1] This refers to the domain that you are scaling.

29.3.2 Mounting Middleware Home and Creating a New Machine when Scaling Out

Before scaling out a component of the OAM application tier, mount the Middleware home and create a new machine.

To mount the Middleware home and create a new machine:

1. On the new node, mount the existing Middleware home, which should include the Oracle Fusion Middleware installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain. See Section 9.11, "Mounting Shared Storage onto the Host." for more information.
2. To attach *IAD_ORACLE_HOME* in shared storage to the local Oracle Inventory, execute the following command:

```
cd IAD_ORACLE_HOME/oui/bin
./attachHome.sh -jreLoc JAVA_HOME
```

> **Note:** This section uses IAD_ORACLE_HOME as an example. Use the same procedure for IGD_ORACLE_HOME.

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *HOME*`/bea/beahomelist` file and add *IAD_MW_HOME*`/oui/bin` to it.
4. Log in to the WebLogic Administration Console for the IAMAccessDomain at the address listed in Section 31.2, "About Identity and Access Management Console URLs."
5. Create a new machine for the new node to be used, and add the machine to the domain, as follows.
   a. Select **Environment -> Machines** from the Navigation menu.
   b. Click **Lock and Edit**.
   c. Click **New** on the Machine Summary screen.
   d. Enter the following information:

      Name: Name of the machine (NEWHOSTn)

      Machine OS: Select UNIX.
   e. Click **Next**.
   f. On the Node Manager Properties page, enter the following information:

      Type: SSL.

      Listen Address: *NEWHOSTn*.
   g. Click **Finish**.
   h. Click **Activate Changes**.

29.3.3 Creating a New Node Manager when Scaling Out

Node Manager is used to start and stop WebLogic managed servers on the new host. In order to create a new node manager for the new host perform the following steps:

1. Create a new directory for the new node manager by copying an existing one. Copy the directory *SHARED_CONFIG*/nodemanager/oamhost1.example.com to: *SHARED_CONFIG*/nodemanager/*newiamhost*.example.com

   For example:

   ```
   cp -r $SHARED_CONFIG/nodemanager/oamhost1.example.com $SHARED_
   CONFIG/nodemanager/newiamhost.example.com
   ```

2. Change to the newly created directory.

   ```
   cd SHARED_CONFIG/nodemanager/NEWHOST3.example.com
   ```

3. Edit the nodemanager.properties file, changing all the entries for OAMHOST1 to OAMHOST3. For example:

   ```
   DomainsFile=/u01/oracle/config/nodemanager/OAMHOST1.example.com/nodemanager.dom
   ain
   ```

   becomes

   ```
   DomainsFile=/u01/oracle/config/nodemanager/NEWHOST3.example.com/nodemanager.dom
   ain
   ```

4. Edit the startNodeManagerWrapper.sh file, changing all the entries for OAMHOST1 to OAMHOST3. For example:

   ```
   NM_HOME=/u01/oracle/config/nodemanager/oamhost1.example.com
   ```

   becomes

   ```
   NM_HOME=/u01/oracle/config/nodemanager/oamhost3.example.com
   ```

5. Start the node manager by invoking the command:

   ```
   ./startNodeManagerWrapper.sh
   ```

6. Update the node manager configuration by following the steps in Chapter 29.5.4, "Updating Node Manager Configuration" to ensure that certificates are created for the new host.

29.3.4 Running Pack/Unpack

Whenever you extend a domain to include a new managed server, you must extract the domain configuration needs from the *ASERVER_HOME* location to the *MSERVER_HOME* location. This applies whether you are scaling up or out. To do this perform the following steps.

> **Note:** The following steps are an example of packing and unpacking the IAMAccessDomain

1. Pack the domain on the host where the administration server is located, for example: OAMHOST1:

   ```
   pack.sh -domain=IAD_ASERVER_HOME -template =/templates/managedServer.jar
   -template_name="template_name" -managed=true
   ```

The pack.sh script is located in *ORACLE_COMMON_HOME*/common/bin.

2. Unpack the domain on the new host for scale out, or on the existing host for scale up, using the command:

```
unpack.sh -domain=IAD_MSERVER_HOME -template=/templates/managedServer.jar -app_
dir=IAD_MSERVER_HOME/applications
```

The unpack.sh script is located in *ORACLE_COMMON_HOME*/common/bin.

3. If you are scaling out, start Node Manager and update the property file.
   a. Start and stop Node Manager as described in Section 31.1, "Starting and Stopping Enterprise Deployment 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 31.1, "Starting and Stopping Enterprise Deployment Components."

29.3.5 Performing Application-Specific Steps

This section contains the following topics:

- Section 29.3.5.1, "Cloning an Existing Managed Server."
- Section 29.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 29.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 29.3.5.3, "Scaling Oracle Identity Manager"
- Section 29.3.5.4, "Updating Oracle Adaptive Access Manager Integration"

29.3.5.1 Cloning an Existing Managed Server

Create a new managed server by cloning an existing managed server of the same type. To scale out/up Access Manager, clone wls_oam1. Similarly, to scale out/up Identity Manager, clone wls_oim1.

The following example is for cloning an Access Manager managed server, although the procedure is the same for all products.

1. Log in to the Oracle WebLogic Administration Console for the domain whose managed server you are cloning, at the address listed in Section 31.2, "About Identity and Access Management Console URLs." For this example the domain is IAMAccessDomain.
2. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
3. Click **Lock & Edit** from the Change Center menu.
4. Select an existing server on the host you want to extend, for example: WLS_OAM1.
5. Click **Clone**.
6. Enter the following information:
   - **Server Name**: A new name for the server, for example: WLS_OAM3.

- **Server Listen Address**: The name of the host on which the Managed Server runs.
- **Server Listen Port**: The port the new Managed Server uses. This port must be unique within the host.

  If you are scaling out, you can use the default port, `14100` (*`OAM_PORT`* in Table 7–1). If you are scaling up, choose a unique port.

7. Click **OK**.
8. Click the newly created server **WLS_OAM3**
9. Set **Machine** to be the machine you created in Section 29.3.2, "Mounting Middleware Home and Creating a New Machine when Scaling Out""
10. Click **Save**.
11. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_OAM3` Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `NEWHOST`.

    If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings were propagated to the cloned server. To disable host name verification:

    a. In Oracle Enterprise Manager Fusion Middleware Control, select **Oracle WebLogic Server Administration Console**.
    b. Expand the **Environment** node in the Domain Structure window.
    c. Click **Servers**. The Summary of Servers page appears.
    d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.
    e. Click the **SSL** tab.
    f. Click **Advanced**.
    g. Set **Hostname Verification** to `None`.
    h. Click **Save**.
12. Click **Activate Changes** from the Change Center menu.

29.3.5.2 Scaling Oracle Access Management Access Manager

This section contains steps specific to scaling Access Manager.

> **Note:** If you are using shared storage, allow the new host access to that shared storage area.

Scale Oracle Access Management Access Manager by performing the steps in the following subsections:

- Section 29.3.5.2.1, "Running Pack/Unpack"
- Section 29.3.5.2.2, "Register Managed Server with Oracle Access Management Access Manager"
- Section 29.3.5.2.3, "Updating WebGate Profiles"

- Section 29.3.5.2.4, "Updating the Web Tier"

29.3.5.2.1 Running Pack/Unpack Run `pack` and `unpack` as described in Section 29.3.4, "Running Pack/Unpack".

29.3.5.2.2 Register Managed Server with Oracle Access Management Access Manager Register the new Managed Server with Oracle Access Management Access Manager. You now must configure the new Managed Server now as an Access Manager server. You do this from the Oracle Access Management Console. Proceed as follows:

1. Log in to the Access Management console at `http://IADADMIN.example.com/oamconsole` as the user you specified during response file creation.
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
   - **Server Name**: `WLS_OAM3`
   - **Host**: Host that the server runs on
   - **Port**: Listen port that was assigned when the Managed Server was created
   - **OAM Proxy Port**: Port you want the Access Manager proxy to run on. This is unique for the host
   - **Proxy Server ID**: `AccessServerConfigProxy`
   - **Mode**: Set to same mode as existing Access Manager servers.
6. Click **Coherence** tab.

   Set **Local Port** to a unique value on the host.
7. Click **Apply**.
8. Restart the WebLogic Administration Server as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components"

29.3.5.2.3 Updating WebGate Profiles Add the newly created Access Manager server to all WebGate Profiles that might be using it, such as `Webgate_IDM`, `Webgate_IDM_11g`, and `IAMSuiteAgent`

For example, to add the Access Manager server to `Webgate_IDM`, access the Access Management console at: `http://IADADMIN.example.com/oamconsole`

Then proceed as follows:

1. Log in as the Access Manager Administrative User.
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
4. Click the open folder icon, then click **Search**.

   You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.

7. Click **+** in the **Primary Server** list (or the **Secondary Server** list if this is a secondary server).
8. Select the newly created managed server from the **Server** list.
9. Set **Maximum Number of Connections** to `10`.
10. Click **Apply**.

Repeat Steps 5 through 10 for **Webgate_IDM_11g**, **IAMSuiteAgent**, and all other WebGates that might be in use.

You can now start the new Managed Server, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components"

29.3.5.2.4 Updating the Web Tier Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 29.3.6, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files"

Save the file and restart the Oracle HTTP server, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components"

29.3.5.3 Scaling Oracle Identity Manager

You already have a node that runs a Managed Server configured with Oracle SOA Suite and Oracle Identity Manager components. The node contains a Middleware home, a SOA Oracle home, an Oracle Identity Manager Oracle home, and a domain directory for existing Managed Servers. Use the existing installations in shared storage for creating a new WLS_SOA and WLS_OIM managed server. There is no need to install the Oracle Identity and Access Management or Oracle SOA Suite binaries in a new location

When scaling up, you add WLS_SOA and WLS_OIM managed servers to existing nodes.

In either case, you must run pack and unpack.

When you scale out the topology, you add new Managed Servers configured with Oracle Identity Manager and SOA to new nodes. First check that the new node can access the existing home directories for WebLogic Server, Oracle Identity Manager, and SOA. You do need to run pack and unpack to bootstrap the domain configuration in the new node.

Follow the steps in the following subsections to scale the topology:

- Section 29.3.5.3.1, "Configuring New JMS Servers"
- Section 29.3.5.3.2, "Performing Pack/Unpack When Scaling Out"
- Section 29.3.5.3.3, "Configuring Oracle Coherence for Deploying Composites"
- Section 29.3.5.3.4, "Enabling Communication for Deployment Using Unicast Communication"
- Section 29.3.5.3.5, "Specifying the Host Name Used by Oracle Coherence"
- Section 29.3.5.3.6, "Completing the Oracle Identity Manager Configuration Steps"

29.3.5.3.1 Configuring New JMS Servers Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server. You do this as follows:

1. Log in to the WebLogic Administration Server in the IAMGovernanceDomain, as described in Section 31.2, "About Identity and Access Management Console URLs," and navigate to **Services -> Messaging -> JMS Servers**.

2. Click **New**.
3. Enter a value for **Name**, such as `BPMJMSServer_auto_3`.
4. Click **Create New Store**.
5. Select `FileStore` from the list
6. Click **Next**.
7. Enter a value for **Name**, such as `BPMJMSFileStore_auto_3`
8. Enter the following values:

   Target: The new server you are creating.

   Directory: *`IGD_ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_3`
9. Click **OK**.
10. When you are returned to the JMS Server screen, select the newly created file store from the list.
11. Click **Next**.
12. On the next screen set the Target to the server you are creating.
13. Click **Finish**.

Create the following JMS Queues depending on the managed server you are creating:

Server	JMS Server Name	File Store Name	Directory	Target
WLS_SOA*n*	BPMJMSServer_auto_*n*	BPMJMSFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	SOAJMSServer_auto_*n*	SOAJMSFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/SOAJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	UMSJMSServer_auto_*n*	UMSJMSFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/UMSJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_OIM*n*	JRFWSAsyncJmsServer_auto_*n*	JRFWSAsyncFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/RFWSAsyncFileStore_auto_`*n*	WLS_OIM*n*
WLS_OIM*n*	OIMJMSServer_auto_*n*	OIMJMSFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/OIMJMSFileStore_auto_`*n*	wls_OIM*n*
WLS_SOA*n*	PS6SOAJMSServer_auto_*n*	PS6SOAJMSFileStore_auto_*n*	*`IGD_ASERVER_HOME`*`/jms/PS6SOAJMSFileStore_auto_`*n*	wls_SOA*n*

Add the newly created JMS Queues to the existing JMS Modules by performing the following steps:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain, at the address listed in Section 31.2, "About Identity and Access Management Console URLs."
2. Navigate to **Services -> Messaging -> JMS Modules**
3. Click a JMSModule, such as **SOAJMSModule**
4. Click the **Sub Deployments** tab.

5. Click the listed sub deployment.

> **Note:** This subdeployment module name is a random name in the form of **JMSServerName*XXXXXX*** resulting from the Configuration Wizard JMS configuration.

6. Assign the newly created JMS server, for example **SOAJMSServer_auto*n***.
7. Click **Save**.
8. Perform this for each of the JMS modules listed in the following table:

JMS Module	JMS Server
BPMJMSModule	BPMJMSServer_auto_*n*
JRFWSAsyncJmsModule	JRFWSAsyncJmServer_auto_*n*
OIMJMSModule	OIMJMSServer_auto_*n*
SOAJMSModule	SOAJMSServer_auto_*n*
UMSJMSSystemResource	UMSJMSServe_auto_*n*

9. Click **Activate Configuration** from the Change Center menu.

29.3.5.3.2 Performing Pack/Unpack When Scaling Out

This section is necessary only when you are scaling out.

Run `pack` and `unpack` as described in Section 29.3.4, "Running Pack/Unpack"

29.3.5.3.3 Configuring Oracle Coherence for Deploying Composites

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Note:** An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

29.3.5.3.4 Enabling Communication for Deployment Using Unicast Communication

Specify the nodes using the `tangosol.coherence.wkan` system property, where `n` is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the

virtual host name used by the SOA server as the listener addresses, for example: SOAHOST3VHN. Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab. You will also need to add the new server to the existing entries.

> **Tip:** To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

> **Note:** SOAHOST3VHN is the virtual host name that maps to the virtual IP where WLS_SOA3 listening (in SOAHOST3).

29.3.5.3.5 Specifying the Host Name Used by Oracle Coherence Use the Administration Console to specify a host name used by Oracle Coherence.

To add the host name used by Oracle Coherence:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (**WLS_SOA1** or **WLS_SOA2**, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Enter the following for WLS_SOA1, WLS_SOA2, and WLS_SOA3 into the Arguments field.

   For WLS_SOA1, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST1VHN
   ```

   For WLS_SOA2, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST2VHN
   ```

   For WLS_SOA3, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST3VHN
   ```

Note: There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the text to your Administration Console's arguments text field. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST1VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST2VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA3 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST3VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

For more information about Coherence Clusters see the *Oracle Coherence Developer's Guide*.

8. Click **Save** and **Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

29.3.5.3.6 Completing the Oracle Identity Manager Configuration Steps 1.Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

From the WebLogic Administration Console, select the **Server_name** > **Configuration** > **Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

2. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOA`*n* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `OIMHOST`*n*. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

   To disable host name verification:

   a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.

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

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

   d. Select **WLS_SOA*n*** in the Names column of the table. The Settings page for the server appears.

   e. Click the **SSL** tab.

   f. Click **Advanced**.

   g. Set **Hostname Verification** to `None`.

   h. Click **Save**.

3. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIM`*n* Managed Servers. In Step d, select **WLS_OIM*n*** in the Names column of the table.

4. Click **Activate Changes** from the Change Center menu.

5. Restart the WebLogic Administration Server as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components"

6. Start and test the new Managed Server from the Administration Console.

   a. Shut down the existing Managed Servers in the cluster.

   b. Ensure that the newly created Managed Server, `WLS_SOA`*n*, is up.

c. Access the application on the newly created Managed Server (`http://vip:port/soa-infra`). The application should be functional.

7. Configure the newly created managed server for server migration. Follow the steps in Chapter 21, "Configuring Server Migration for an Enterprise Deployment." to configure server migration.

Note: Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP addresses for the new Managed Servers are already present in the new node.

---

8. Test server migration for this new server. Follow these steps from the node where you added the new server:

   a. Stop the `WLS_SOA`*n* Managed Server.

      To do this, run:

      ```
      kill -9 pid
      ```

      on the process ID (PID) of the Managed Server. You can identify the PID of the node using

      ```
      ps -ef | grep WLS_SOAn
      ```

   b. Watch the Node Manager Console. You should see a message indicating that the floating IP address for WLS_SOA1 has been disabled.

   c. Wait for the Node Manager to try a second restart of WLS_SOA*n*. Node Manager waits for a fence period of 30 seconds before trying this restart.

   d. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.

   e. Repeat Steps a-d for WLS_OIM*n*.

29.3.5.4 Updating Oracle Adaptive Access Manager Integration

If you have extended your domain with Oracle Adaptive Access Manager and have integrated Oracle Identity Manager with Oracle Adaptive Access Manager, you must update Oracle Adaptive Access Manager so that it is aware of the new Oracle Identity Manager server.

29.3.6 Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files

Scaling an Application Tier component typically requires you to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

In the Web tier, there are several configuration files under *`WEB_ORACLE_INSTANCE`*`/config/OHS/componentname/moduleconf`, including `admin_vh.conf`, `sso_vh.conf` and `igdinternal_vh.conf`. Each contain a number of entries in location

blocks. If a block references two server instances and you add a third one, you must update that block with the new server.

For example if you add a new Access Manager server, you must update `sso_vh.conf` to include the new managed server. You add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.example.com:14100,OAMHOST2.example.com:14100
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.example.com:14100,OAMHOST2.example.com:14100
</Location>
```

to:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.example.com:14100,OAMHOST2.example.com:14100,OAMHOST1.example.com:14101
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.example.com:14100,OAMHOST2.example.com:14100,OAMHOST3.example.com:14100
</Location>
```

Once you have updated the configuration file, restart the Oracle HTTP server(s) as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components." Oracle recommends that you do this sequentially to prevent loss of service.

29.4 Scaling the Web Tier

The Web Tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance.

To scale the Oracle HTTP Server, perform the steps in the following subsections:

- Section 29.4.1, "Assembling Information for Scaling the Web Tier."
- Section 29.4.2, "Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out."
- Section 29.4.3, "Running the Configuration Wizard to Configure the HTTP Server."
- Section 29.4.4, "Registering Oracle HTTP Server with WebLogic Server."
- Section 29.4.5, "Reconfiguring the Load Balancer."

29.4.1 Assembling Information for Scaling the Web Tier

Assemble the following information before scaling the Web Tier.

Description	Variable	Documented Value	Customer Value
Host name		WEBHOST1.example.com	

Description	Variable	Documented Value	Customer Value
OHS port	*WEB_HTTP_PORT*	7777	
Instance Name	webn	web1 or web2	
Component Name	webn	web1 or web2	
WebLogic Administration Host, IAMAccessDomain	*IADADMINVHN*	IADADMINVHN.example.com	
Access Management WLS Server Port	*IAD_WLS_PORT*	7001	
WebLogic Administrative User		weblogic_idm	
WebLogic Administrative Password			

29.4.2 Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out

On the new node, mount the existing Middleware home.

Copy all files created in *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf from the existing Web Tier configuration to the new one.

29.4.3 Running the Configuration Wizard to Configure the HTTP Server

Perform these steps to configure the Oracle Web Tier:

1. Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the file stage/Response/staticports.ini. Copy it to a file called ohs_ports.ini. Delete all entries in ohs_ports.ini except for OHS PORT and OPMN Local Port. Change the value of OPMN Local Port to 6700. If you are scaling out, you can use the default value, 7777, for OHS PORT. If you are scaling up, you must choose a unique value for that instance on the machine.

   Note: If the port names in the file are slightly different from OHS PORT and OPMN Local Port, use the names in the file.

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

   ```
   cd WEB_ORACLE_HOME/bin
   ```

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

   Ensure that Associate Selected Components with WebLogic Domain is selected.

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

   Click **Next**.
3. On the Specify WebLogic Domain Screen, enter

- **Domain Host Name**: `IADADMINVHN.example.com`
- **Domain Port No**: `7001`, where `7001` is *IAD_WLS_PORT* in Section 8.1, "Summary of Virtual IP Addresses Required."
- **User Name**: Weblogic Administrator User (For example: `weblogic`)
- **Password**: Password for the Weblogic Administrator User account

Click **Next**.

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

   Enter the following values for WEBHOST*n*, where *n* is the number of the new host, for example, `3`:

   - **Instance Home Location**: *WEB_ORACLE_INSTANCE*, for example: `/u02/local/oracle/config/instances/ohs1`
   - **Instance Name**: `webn`
   - **OHS Component Name**: `webn`

   Click **Next**.

5. On the Configure Ports screen, you use the `ohs_ports.ini` file you created in Step 1to specify the ports to be used. This enables you to bypass automatic port configuration.

   a. Select **Specify Ports using a Configuration File**.

   b. In the file name field specify `ohs_ports.ini`.

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

6. On the Specify Security Updates screen, specify these values:

   - **Email Address**: The email address for your My Oracle Support account.
   - **Oracle Support Password**: The password for your My Oracle Support account.

   Select: **I wish to receive security updates via My Oracle Support**.

   Click **Next**.

7. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

   Click **Configure**.

   On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

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

29.4.4 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the new Oracle HTTP server, you must register the Oracle HTTP server with IAMAccessDomain. To do this, register Oracle HTTP Server with WebLogic Server by running the following command on the host where the new server is running:

```
cd WEB_ORACLE_INSTANCE/bin
./opmnctl registerinstance -adminHost IADADMINVHN.example.com \
   -adminPort WLS_ADMIN_PORT -adminUsername weblogic
```

29.4.5 Reconfiguring the Load Balancer

Add the new Oracle HTTP Server instance to the existing server pool defined on the load balancer for distributing requests across the HTTP instances.

29.4.6 Scaling Up Oracle Traffic Director

To scale up Oracle traffic director:

1. Install Oracle Traffic Director on the new host as described in Section 11.2.2, "Installing Oracle Traffic Director."
2. Create a new instance of Oracle Traffic Director on the new host as described in Section 14.2.2, "Registering WEBHOST2 with the Administration Node."
3. Deploy the configuration to the new node by following the instructions in Section 14.2.9, "Deploying the Configuration and Testing the Virtual Server Addresses."
4. Create a new failover group for the new Oracle Traffic Director instance as described in Section 14.2.10, "Creating a Failover Group for Virtual Hosts."
5. Add the new Oracle Traffic Director failover group to the hardware load balancer pool.

29.4.7 Scaling Oracle Mobile Security Access Server

This section describes how to scale the Oracle Mobile Security Access Server.

This section contains the following topics:

- Section 29.4.7.1, "Installing Oracle Mobile Security Access Server"
- Section 29.4.7.2, "Configuring MSAS Gateway Instance"
- Section 29.4.7.3, "Creating an MSAS Configuration Property File"
- Section 29.4.7.4, "Configuring the MSAS Instance Using configMSAS.sh"
- Section 29.4.7.5, "Validating the MSAS Configuration"
- Section 29.4.7.6, "Integrating MSAS with the Identity Store"
- Section 29.4.7.7, "Starting MSAS Instances on OHSHOST1 and OHSHOST2"

29.4.7.1 Installing Oracle Mobile Security Access Server

This section explains how to install Oracle Mobile Security Access Server (MSAS) on OHSHOST1 and OHSHOST2.

As described in Preparing File System Chapter, you install the Oracle MSAS onto a private disk.

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

- LD_ASSUME_KERNEL
- ORACLE_INSTANCE

To start the Oracle Universal Installer:

1. On Linux, run the following command:

```
./runInstaller -jreLoc JAVA_HOME
```

2. On the Specify Inventory Directory screen, do the following:
   a. Enter *HOME*`/oraInventory`, where *HOME* is the home directory of the user performing the installation (this is the recommended location).
   b. Enter the OS group for the user performing the installation and click **Next**.
   c. Follow the instructions on screen to execute `createCentralInventory.sh` as root and click **OK**.
3. On the Welcome screen, click **Next**.
4. On the Install Software Updates Screen choose to either search for updates, and click **OK**, or select **Skip Software Updates** and click **Next**.
5. On the Prerequisite Checks screen, if all the pre-checks have completed successfully, click **Next**.
6. On the Specify Installation Location screen, specify the following values:
   - **Fusion Middleware Home Location (Installation Location)**: For example: `/u01/oracle/products/web`
   - **Oracle Home Location Directory**: `omsas`

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

29.4.7.2 Configuring MSAS Gateway Instance

After installation, you must configure the MSAS gateway instance. Each instance must be configured exactly the same, with the same instance ID, so that they can function as a cluster. While this can be done interactively, it is better to do so by using a property file, which can then be used to configure each instance.

29.4.7.3 Creating an MSAS Configuration Property File

You can use the file created by provisioning at the following location:

```
LCM_HOME/provisioning/logs
```

Create a property file called `msas_instance.props` with the following information:

```
MSM_URL: http://iadinternal.example.com:80
MSM_USER_NAME:  weblogic
MSAS_INSTANCE_ID: gateway1
MSAS_INSTANCE_DIR:  LOCAL_CONFIG_DIR/instances/
MSAS_INSTANCE_SSL_PORT: 14191
OAM_HOST: iadadminvhn.example.com
OAM_PORT: 7001
OAM_USER_NAME: iadadmin
OAM_PROTECT: /
OAUTH_HOST: login.example.com
OAUTH_PORT: 443
OAUTH_IS_SSL: true
OAUTH_SP_ENDPOINT: /oauthservice
OAM_COOKIE_DOMAIN: .example.com
MSAS_LBR_URL: https://msas.example.com
```

Property Descriptions:

- **MSM_URL** is the URL of the Oracle HTTP Server which directs requests to the MSM managed servers. For example:

  `http://iadinternal.example.com:80`

  This is the URL which is used for internal call backs.
- **MSM_USER_NAME** is the domain administrator name. For example: `weblogic`.
- **MSAS_INSTANCE_ID** is the collective name of the instance. It can be any string, but must be consistent across instances. This must be the same as the value provided as input to the provisioning wizard.
- **MSAS_INSTANCE_DIR** is where the instance configuration files are created. For example:

  `LOCAL_CONFIG_DIR``/instances`
- **MSAS_INSTANCE_PORT** is the port on which MSAS listens for requests. This port is SSL enabled.
- **OAM_HOST** is the `IAMAccessDomain` Administration Server Virtual Host. For example:

  `IADADMINVHN.example.com`
- **OAM_PORT** is the Port used by the `IAMAccessDomain` Administration Server. For example: `7001`
- **OAM_USER_NAME** This is the `OAMAdmin` account you created previously.
- **OAM_PROTECT** Specifies the resource pattern for each protected application, for example, `/myapp/login`. The pattern you enter is relative to the host and port of the OAM gateway. This entry must begin with a `/`.

  You can enter `/`, which means that any requesting URL ending in `/` is protected.
- **OAUTH_HOST** is the `OAUTH` entry point in an enterprise deployment. This is the load balancer name. For example, `login.example.com`.
- **OAUTH_PORT** is the port that OAM Managed Servers use in an enterprise deployment. This is the load balancer port. For example, `443`.
- **OAUTH_IS_SSL** specifies where `OAUTH` is using the SSL or non SSL port. Valid values are: `true/false`. In an enterprise deployment the value is `true`.
- **OAUTH_SP_ENDPOINT** is the endpoint where you access clients from the `OAUTH` server, for example: `/oauthservice`
- **MSAS_LBR_URL** is the load balancer entry point for MSAS. For example, `https://`*`msas.example.com`*`:443`

29.4.7.4 Configuring the MSAS Instance Using configMSAS.sh

Once you have created the property file, run the `configMSAS.sh` script to configure the instance. This script is located in the following directory:

`MSAS_ORACLE_HOME``/bin`

To execute the script use the following command:

`MSAS_ORACLE_HOME``/bin/configMSAS.sh -properties msas_instance.props`

You are prompted for the following:

- The mobile security manager password. This is the WebLogic Administrator password of the `IAMAccessDomain`
- The OAM Administrator password.

29.4.7.5 Validating the MSAS Configuration

The `configMSAS.sh` command creates an MSAS instance in the following directory:

LOCAL_CONFIG_DIR`/instances/`*gateway-id*

Where the `gateway-id` is the value you provided in the property file. Validate that this directory exists.

If the directory exists you can validate that the instance has been registered with MSM by doing the following:

1. Log in to the Access Console as the `oamadmin` user.
2. On the Launch Pad, click the **Mobile Security** button at the top of the screen.
3. Click **Environments** in the **Mobile Security Access Server** section, the MSAS instances appear.
4. Click the **MSAS** title.

   The **EDGMSAS** instance appears.

> **Note:** Due to a known issue, once you have registered the second instance, only one MSAS instance appears, which is the second instance. This is a cosmetic error and has no impact on system functionality.

29.4.7.6 Integrating MSAS with the Identity Store

This section describes how to integrate MSAS with the Identity Store.

To integrate MSAS with the Identity Store on OAMHOST1:

1. Set the environment variables MW_HOME, JAVA_HOME, ORACLE_HOME and WL_HOME
   - Set MW_HOME to *IAD_MW_HOME*.
   - Set JAVA_HOME to *JAVA_HOME*.
   - Set ORACLE_HOME to *IAD_ORACLE_HOME*.
   - Set WL_HOME to *IAD_MW_HOME*`/wlserver_10.3`
2. Run the `idmConfigTool` utility to perform the integration.

   The syntax of the command on Linux is:

   ```
   cd IAD_ORACLE_HOME/idmtools/bin
   idmConfigTool.sh -configOMSS mode=OMSAS input_file=configfile
   ```

   For example:

   ```
   idmConfigTool.sh -configOMSS mode=OMSAS input_file=msas.props
   ```

   When the command runs, you are prompted to enter the password of the account with which you are connecting to the Identity Store. You are also asked to specify the passwords you want to assign to:

- **OMSS Keystore**: This is the password that is assigned to the OMSS keystore when it is created.
- **SCEP Dynamic Challenge Password**
- The schema password for the RCU schema `EDGIAD_OMSM`.

3. 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.
4. This process creates objects in the domain, in order for these objects to be visible the Administration Server must be restarted.
5. Pack and unpack the `IAMAccessDomain` as described in Section 29.3.4, "Running Pack/Unpack". Creating a Separate Domain Directory for Managed Servers. Unpack to both OAMHOST1 and OAMHOST2.
6. Restart WebLogic Administration console, WLS_OAM1, WLS_OAM2, WLS_AMA1, WLS_AMA2.

29.4.7.7 Starting MSAS Instances on OHSHOST1 and OHSHOST2

Once you have configured the instances, you can start them. To start the instances issue the following command:

```
MSAS_INSTANCE_HOME/bin/startServer.sh
```

The MSAS instances should start without error.

29.5 Post-Scaling Steps for All Components

Perform the following post-scaling steps.

- Section 29.5.1, "Adding a New Managed Server to the Oracle Traffic Director Server Pool."
- Section 29.5.2, "Updating the Topology Store."
- Section 29.5.3, "Updating Stop/Start Scripts."
- Section 29.5.4, "Updating Node Manager Configuration."

29.5.1 Adding a New Managed Server to the Oracle Traffic Director Server Pool

The procedures described in this section show you how to add a new managed server or directory instance to an existing OTD server pool.

The following example is for OAM, but the process is the same for all managed servers/directory instances.

To add a third instance to the Oracle Traffic Director Access Manager server pool:

1. Log into the Oracle Traffic Director Administration Console.
2. Click **Server Pools** on the left panel.
3. Click the pool name, for example: **origin-server-pool-1**.
4. On the right panel, click **New Origin Server**.
5. Add the new Managed Server/Directory Instance, for example: **IAMHOST3, 14100** of the Origin Server.

   Click **Next**.
6. Click **New Origin Server**, and then **Close**.

7. Click **Deploy Changes** on the top of the panel.

29.5.2 Updating the Topology Store

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Life Cycle Tools read the store in order to build and execute the patch plan. If you scale out/up the topology you must add new entries to the store covering the new additions to the deployment.

29.5.3 Updating Stop/Start Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. When you create a new managed server in the domain you need to update the domain configuration so that these start and stop scripts can also start the newly created managed server.

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

29.5.4 Updating Node Manager Configuration

Update the node manager configuration, as described in the following sections:

- Section 29.5.4.1, "Starting and Stopping Node Manager."

29.5.4.1 Starting and Stopping Node Manager

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

`newmachine``.example.com NM` *`nodemanager_pathname nodemanager_port`*

For example:

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

If you want to start a managed server called WLS_OIM3 add an entry which looks like this:

`newmachine``.example.com OIM` *`ManagedServerName`*

For example:

```
OAMHOST3 OIM WLS_OIM3
```

Save the file.

If you added a new node manager, you must enable it for SSL as described in Chapter 16, "Setting Up Node Manager for an Enterprise Deployment".

30

Topology Tool Commands for Scaling

This chapter describes the topology tool commands for scaling.

When you provision your environment using LCM, it creates a map of the topology in a file called `topology.xml` which is used for automated patching. If you scale out your environment using the procedures in Chapter 29, "Scaling Enterprise Deployments", you need to ensure that these changes are reflected in the topology file. You can do this using the commands in this chapter.

This chapter contains the following sections:

- Overview of Topology Tool Commands for Scaling
- Syntax of the Topology Tool
- Commonly-Used Command Line Operations
- Steps and Command-Line Examples

30.1 Overview of Topology Tool Commands for Scaling

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Life Cycle Tools read the store in order to build and execute the patch plan.

Chapter 29, "Scaling Enterprise Deployments" describes how to scale the deployment up or out using a variety of tools. As part of a scaling procedure, you must add new entries to the store covering the new additions to the deployment. This is done using the IAM Topology Tool.

The tool is located at: *IDMLCM_HOME*`/topotool/bin`

Before running the Topology Tool, back up your entire *LCM_ROOT*`/lcmconfig/topology` directory.

> **Note:** Many of the command-line options use instance or component names that include numbers, for example `OUD3`. You should already have determined these names when you assembled information for scaling. See the Assembling Information sections in Chapter 29, "Scaling Enterprise Deployments".

30.2 Syntax of the Topology Tool

The general syntax is:

`topotool.sh` *command* `[-option]`

For help, use:

```
topotool.sh [-help]

topotool.sh command [-help]
```

Note: This section is not a complete description of the syntax of the Topology Tool. The commands and options listed in this section include only those that are used in this guide.

30.2.1 Commands

Add

Adds information to the topology store.

```
topotool.sh add [options]
```

Modify

Modifies information in the topology store.

```
topotool.sh modify [options]
```

30.2.2 Command-Line Options Used with Add

-component

Specifies adding of a component.

-confighomename oud*n* | oim*n* | oam*n* | soa*n* | NodeManager:Access | NodeManager:Identity | ohs*n*

Specifies a local or shared configuration home to add. Used with `-instance`.

-dbname *DBNAME*

Specifies the Oracle Database to use. Used with `-instance`. In this guide, *DBNAME* is always `OIM:DB`.

-description *STRING*

Used with `-machine` and `-confighome`. *STRING* is a quoted string, such as `"oim3 machine"`.

-fqdn *HOSTNAME*

Specifies a host. The *HOSTNAME* format is a fully qualified domain name, such as `ldaphost3.example.com`, `oimhost4.example.com`. Used with `-host`.

-hometype OUD | IAM | SOA | WEBTIER

Specifies the home type to be added. Used with `-instance`.

-host

Specifies adding a host.

-instance

Specifies adding an instance.

-instancegroup *STRING*

Specifies an instance group. In this guide, *STRING* is always `1` when used with `-instancegroup`. Used with `-instance`.

-machine

Specifies adding a machine

-machinename *MACHINE*

Specifies the machine to be added. Used with `-instance` and `-machine`. The format of *MACHINE* is a fully qualified machine name such as `ldaphost3.example.com`, `oimhost4.example.com`.

-mwhomename Directorytier:MW_HOME | Access:MW_HOME | Identity:MW_HOME | Webtier:MW_HOME | Webtier:MW_HOME_2 | Webtier:MW_HOME_*n*

Specifies the Middleware home to add. Used with `-instance`

-name *NAME*

Specifies the name of a machine or an instance. When used with `-machine`, the *NAME* format is a fully-qualified hostname, such as `ldaphost3.example.com`.

When used with `-instance` or `-confighome`, the *NAME* format is *`productn`*, for example `oid3`.

When used with `-instance`, the *NAME* format is a hostname and port pair, in the format *`productn`*`:`*`host`*`:plain` for a non-SSL port and *`productn`*`:`*`host`*`:ssl` for an SSL port, where *`product`* is a component, such as `OUD` or `OIM`, and *`n`* is the instance number.

When used to add an OPMN instance the hostname part of the *NAME* format is `OPMN`, for example: `OPMN:webhost3:ssl`.

-path *PATH*

Specifies a quoted directory path, such as `"/u01/oracle/config/nodemanager/oimhost3.example.com"`. Used with `-confighome`

-port *PORT*

Specifies a port number, such as 5556. Used with `-host`.

-secure true | false

Set to `true` for an SSL port and `false` for a non-SSL port. Used with `-host`.

-shared true | false

used with `-confighome` to indicate whether this is a shared or local configuration home.

-sharedlcmconfigaccessible true | false

Specifies whether the shared LCM configuration is accessible. Used with `-machine`. In this guide, it is set to `true` when adding application tier machines and to `false` for web tier machines.

-tier DIRECTORY | IDM | WEB |

Specifies the tier, as listed in Chapter 29, "Scaling Enterprise Deployments".

-type TYPE

Specifies the type of an instance or a component. In both cases, **TYPE** stands for the specific type definition to be used, matching the instance or component being added.

When used with `-instance`, the value can be one of: OUD | OHS_HTTPD | OPMN WLS_ADMIN | WLS_MANAGED | WLS_NODE_MANAGER

When used with `-component`, the value can be one of: OHS_WEBGATE | WLS_ADMIN_OAM_CONSOLE | WLS_ADMIN_WLS_CONSOLE | WLS_MANAGED_OAM | WLS_MANAGED_OIM | WLS_MANAGED_SOA

-virtual true | false

Specifies whether the host being added is a virtual host. Used with `-host`. It is always `false` in this guide.

30.2.3 Command-Line Options Used with Modify for Updating Load Balancer Mappings

-lbrmapping

Specifies modification of the load balancer mapping by the addition of a new host

-lbrname *LBRNAME*

Used with `-lbrmapping`. Specifies the name of the load balancer. *`LBRNAME`* is always `LBR1` or `LBR2` in this guide.

-name idstore | idstore_ssl

Used with `-lbrmapping`. Specifies the load balancer mapping name.

-physicalhosts *HOSTS*

Used with `-lbrmapping`. Specifies a host or a comma-separated list of hosts. For a non-SSL host, the format is *`productn`*`:`*`host`*, for example: `OUD:LDAP:oud1:ldaphost1,oud2:ldaphost2,oud3:ldaphost3`. For an SSL host, the format is *`productn`*`:`*`host`*`:ssl`, for example: oud3:ldaphost3:ssl

30.3 Commonly-Used Command Line Operations

Adding a Machine:

```
topotool.sh add -machine -name MACHINE -sharedlcmconfigaccessible true_false
```

Adding a Non-SSL Host:

```
topotool.sh add -host -name HOST -fqdn FQDN -port PORT -secure false -virtual
false
```

Adding an SSL Host:

```
topotool.sh add -host -name HOST_SSL -fqdn FQDN -port SSL_PORT -secure false
-virtual false
```

Adding a Local Configuration Home:

```
topotool.sh add -confighome -name LOCAL_CONFIG -path PATH -shared false
```

Adding a Shared Configuration Home:

```
topotool.sh add -confighome -name SHARED_CONFIG -path
"/u01/oracle/config/instances/oud3" -shared true
```

Adding an Instance:

```
topotool.sh add -instance -machinename MACHINE -name INSTANCE -type TYPE -tier
TIER -mwhomename MWHOME-hometype  -confighomename  LOCAL_OR_SHARED_CONFIG
-instancegroup 1
```

Adding a Component:

```
topotool.sh add -component -instancename INSTANCE -type TYPE -hosts HOST
```

Updating Load Balancer Mappings:

```
topotool.sh modify -lbrmapping -lbrname LBR -name LBR_MAPPING -physicalhosts HOST
topotool.sh modify -lbrmapping -lbrname LBR_SSL -name LBR_MAPPING -physicalhosts
HOST_SSL
```

30.4 Steps and Command-Line Examples

This section contains notes about each tier, general steps for scaling out the components in that tier, and example command lines. It contains the following topics:

- Section 30.4.1, "Scaling Out / Scaling Up of Directory Tier"
- Section 30.4.2, "Scaling Out / Scaling Up of Application Tier"
- Section 30.4.3, "Scaling Out / Scaling Up of Web Tier"

> **Note:** Do not use the examples directly. You must substitute the values with your own data.

30.4.1 Scaling Out / Scaling Up of Directory Tier

The following sections provide information about scaling the directory tier.

- Section 30.4.1.1, "Directory Tier Notes"
- Section 30.4.1.2, "Topology Tool Steps for Scaling Oracle Unified Directory"
- Section 30.4.1.3, "Scale Out Commands for Oracle Unified Directory"
- Section 30.4.1.4, "Scale Up Commands for Oracle Unified Directory"

30.4.1.1 Directory Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the LDAP hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.

- Reconfigure load balancer mappings.

30.4.1.2 Topology Tool Steps for Scaling Oracle Unified Directory

1. Add a machine with `sharedlcmconfigaccessible` set to true. (Only for scale out).
2. Add a non-SSL host if Oracle Unified Directory is listening on non-SSL port.
3. Add a SSL host if Oracle Unified Directory is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type OUD, tier DIRECTORY, hometype OUD using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Update the load balancer mappings with the newly created non-SSL or SSL hosts.

30.4.1.3 Scale Out Commands for Oracle Unified Directory

- Adding new machine

```
topotool.sh add -machine -name ldaphost3.example.com -description "oud3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.example.com
-port 1389 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn ldaphost3.example.com
-port 1390 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oud3 -description "oud3 local
configuration home" -path "/u02/private/oracle/config/instances/oud3"
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oud3 -description "oud3 configuration
home" -path "/u01/oracle/config/instances/oud3" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename ldaphost3.example.com -name oud3
-description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
HOME -hometype OUD -confighomename oud3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
oud3:ldaphost3,oud3:ldaphost3:ssl
```

- Adding the new host to the load balancer mappings

- Non-SSL:

```
topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
oud3:ldaphost3
```

- SSL:

```
topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
-physicalhosts oud3:ldaphost3:ssl
```

30.4.1.4 Scale Up Commands for Oracle Unified Directory

- Adding new machine

```
topotool.sh add -machine -name ldaphost3.example.com -description "oud3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.example.com
-port 1389 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn ldaphost3.example.com
-port 1390 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oud3 -description "oud3 local
configuration home" -path "/u02/private/oracle/config/instances/oud3"
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oud3 -description "oud3 configuration
home" -path "/u01/oracle/config/instances/oud3" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename ldaphost3.example.com -name oud3
-description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
HOME -hometype OUD -confighomename oud3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
oud3:ldaphost3,oud3:ldaphost3:ssl
```

- Adding the new host to the load balancer mappings
  - Non-SSL:

```
topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
oud3:ldaphost3
```

  - SSL:

```
topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
-physicalhosts oud3:ldaphost3:ssl
```

30.4.2 Scaling Out / Scaling Up of Application Tier

The following sections provide information about scaling the application tier.

30.4.2.1 Application Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.
- Node manager added in case of Scale Out.

30.4.2.2 Topology Tool Steps for OAM

1. Add a machine with `sharedlcmconfigaccessible` set to `true`. (Only for scale out).
2. Add a non-SSL host if OAM is listening on non-SSL port.
3. Add a SSL host if OAM is listening on SSL port.
4. Add a host for OAP.
5. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
6. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
7. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
8. Add a component for the newly created instance of type WLS_MANAGED_OAM using the newly created non-SSL or SSL hosts.

30.4.2.3 Scale Out Commands for OAM

- Adding new machine

```
topotool.sh add -machine -name oamhost3.example.com -description "oam3 machine"
-sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

    ```
    topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.example.com -port
    14100 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.example.com
    -port 14101 -secure true -virtual false
    ```

- Adding the new host for OAP (hostname + port combination)

  ```
  topotool.sh add -host -name oam3:slc03oap3 -fqdn oamhost3.example.com -port
  5575 -secure false -virtual false
  ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oam3 -description "oam3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oam3 -description "oam3 shared
    configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
    -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oamhost3.example.com -name oam3
  -description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
  -hometype IAM -confighomename oam3 -dbname OIM:DB -domainname  IAMAccessDomain
  -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
  oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

  topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
  oam3:oamhost3,oam3:oamhost3:ssl
  ```

30.4.2.4 Scale Up Commands for OAM

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

    ```
    topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.example.com -port
    14100 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.example.com
    -port 14101 -secure true -virtual false
    ```

- Adding new config home

- Local config:

```
topotool.sh add -confighome -name oam3 -description "oam3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
```

- Shared config:

```
topotool.sh add -confighome -name oam3 -description "oam3 shared
configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.example.com -name oam3
-description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
-hometype IAM -confighomename oam3 -dbname OIM:DB -domainname  IAMAccessDomain
-instancegroup 1
```

- Adding component

```
topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
oam3:oamhost3,oam3:oamhost3:ssl
```

30.4.2.5 Topology Tool Steps for OIM

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if OIM is listening on non-SSL port.
3. Add a SSL host if OIM is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_OIM using the newly created non-SSL or SSL hosts.

30.4.2.6 Scale Out commands for OIM

- Adding new machine

```
topotool.sh add -machine -name oimhost3.example.com -description "oim3 machine"
-sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

```
topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.example.com -port
14000 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.example.com
-port 14001 -secure true -virtual false
```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.example.com -name oim3
  -description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
  oim3:oimhost3,oim3:oimhost3:ssl

  topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
  oim3:oimhost3,oim3:oimhost3:ssl
  ```

30.4.2.7 Scale Up commands for OIM

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.example.com -port
    14000 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.example.com
    -port 14001 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.example.com -name oim3
  -description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

```
topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
oim3:oimhost3,oim3:oimhost3:ssl

topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
oim3:oimhost3,oim3:oimhost3:ssl
```

30.4.2.8 Topology Tool Steps for SOA

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if SOA is listening on non-SSL port.
3. Add a SSL host if SOA is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype SOA using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_SOA using the newly created non-SSL or SSL hosts.

30.4.2.9 Scale Out commands for SOA

- Adding new machine

```
topotool.sh add -machine -name oimhost3.example.com -description "soa3 instance
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

```
topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.example.com -port
8001 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.example.com
-port 8002 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name soa3 -description "soa3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name soa3 -description "soa3 shared
configuration home" -path "
/u01/oracle/config/domains/IAMGovernanceDomain"-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.example.com -name soa3
```

```
-description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
IAMGovernanceDomain -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
soa3:oimhost3,soa3:oimhost3:ssl

topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
soa3:oimhost3,soa3:oimhost3:ssl
```

30.4.2.10 Scale Up Commands for SOA

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

```
topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.example.com -port
8001 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.example.com
-port 8002 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name soa3 -description "soa3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name soa3 -description "soa3 shared
configuration home" -path "
/u01/oracle/config/domains/IAMGovernanceDomain"-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.example.com -name soa3
-description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
IAMGovernanceDomain -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
soa3:oimhost3,soa3:oimhost3:ssl

topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
soa3:oimhost3,soa3:oimhost3:ssl
```

30.4.2.11 Steps for Adding Node Manager Steps for OAM/OIM/SOA Scale Out Only

1. Add a non-SSL host if Node Manager is listening on non-SSL port.
2. Add a SSL host if Node Manager is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.

4. Add an instance of type WLS_NODE_MANAGER, tier IDM, hometype IAM using an existing middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
6. Add a component for the newly created instance of type WLS_NODE_MANAGER using the newly created non-SSL or SSL hosts.

30.4.2.12 Commands for Adding NodeManager for Scale Out of OAM

- Adding new host (hostname + port combination) for Node Manager OAM
  - Non-SSL:

    ```
    topotool.sh add -host -name NodeManager:oamhost3 -fqdn oamhost3.example.com
    -port 5556 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name NodeManager:oamhost3:ssl -fqdn
    oamhost3.example.com -port 5556 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name NodeManager:Access -description "node
    manager local configuration home" -path
    "/u01/oracle/config/nodemanager/oamhost3.example.com" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name NodeManager:Access -description " node
    manager shared configuration home " -path
    "/u01/oracle/config/nodemanager/oamhost3.example.com" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oamhost3.example.com -name
  NodeManager:Access -description "node manager  instance" -type WLS_NODE_MANAGER
  -tier IDM -mwhomename Access:IAD_MW_HOME -hometype IAM -confighomename
  NodeManager:Access  -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename NodeManager:Access -type DEFAULT
  -hosts NodeManager:oamhost3, NodeManager:oamhost3:ssl
  ```

30.4.2.13 Commands for Adding NodeManager for Scale Out of OIM

- Adding new host (hostname + port combination) for Node Manager OIM
  - Non-SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3 -fqdn oimhost3.example.com
    -port 5556-secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
    oimhost3.example.com -port 5556 -secure true -virtual false
    ```

- Adding new config home

- Local config:

```
topotool.sh add -confighome -name NodeManager:Identity -description "node
manager local configuration home" -path
"/u01/oracle/config/nodemanager/oimhost3.example.com" -shared false
```

- Shared config:

```
topotool.sh add -confighome -name NodeManager:Identity -description " node
manager shared configuration home " -path
"/u01/oracle/config/nodemanager/oimhost3.example.com" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.example.com -name
NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
-confighomename NodeManager:Identity  -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
-hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
```

30.4.2.14 Commands for Adding NodeManager for Scale Out of SOA

- Adding new host (hostname + port combination) for Node Manager SOA
  - Non-SSL:

```
topotool.sh add -host -name NodeManager:oimhost3 -fqdn oimhost3.example.com
-port 5556-secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
oimhost3.example.com -port 5556 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name NodeManager:Identity -description "node
manager local configuration home" -path
"/u01/oracle/config/nodemanager/oimhost3.example.com" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name NodeManager:Identity -description " node
manager shared configuration home " -path
"/u01/oracle/config/nodemanager/oimhost3.example.com" -shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oimhost3.example.com -name
NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
-confighomename NodeManager:Identity  -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
-hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
```

30.4.3 Scaling Out / Scaling Up of Web Tier

The following sections provide information about scaling the web tier.

30.4.3.1 Web Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries not shared. They are local.
- The config directory is not mounted.
- Reconfigure Load Balancer.

30.4.3.2 Topology Tool Steps for Scaling OHS

1. Add a machine with sharedlcmconfigaccessible set to false. (Only for scale out).
2. Add a non-SSL host if OHS is listening on non-SSL port.
3. Add a SSL host if OHS is listening on SSL port.
4. Add a new Middleware Home with shared set as false. (Only for scale out)
5. Add a new Oracle Home. (Only for scale out)
6. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
7. Add an instance of type OHS_HTTPD, tier WEB, hometype WEBTIER using the newly created middleware home or existing middleware home in case of scale up.
8. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
9. Add a component for the newly created instance of type OHS_WEBGATE using the newly created non-SSL or SSL hosts.
10. Update the SSO, IGDINTERNAL, OIMADMIN, OAMADMIN load balancer mappings with the newly created non-SSL or SSL hosts.

30.4.3.3 Scale Out Commands for Web

- Adding new machine

```
topotool.sh add -machine -name webhost3.example.com -description "ohs3 machine"
-sharedlcmconfigaccessible false
```

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.example.com -port
7777 -secure false -virtual false
```

- SSL:

```
topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.example.com
-port 7778 -secure true -virtual false
```

- Adding new MW Home(s)

```
topotool.sh add -mwhome -name Webtier:WEB_MW_HOME -path
/u01/oracle/products/ohs/ -shared false
```

- Adding new Oracle Home(s)

```
topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type ORACLE_COMMON -path
/u01/oracle/products/ohs/oracle_common

topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type WEBTIER -path
/u01/oracle/products/ohs/ohs

topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type OAM_WG -path
/u01/oracle/products/ohs/webgate
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name ohs3 -description "ohs3 local
configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name ohs3 -description "ohs3 shared
configuration home" -path " /u02/private/oracle/config/instances/ohs3"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename webhost3.example.com -name ohs3
-description "ohs3 instance" -type OHS_HTTPD -tier WEB -mwhomename Webtier:WEB_
MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
ohs3:webhost3,ohs3:webhost3:ssl
```

- Adding the new host to the load balancer mappings
  - Adding to sso load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

  - Adding to igdinternal load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name
igdinternal-physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
```

  - Adding to oimadmin load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

- Adding to oamadmin load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

30.4.3.4 Scale Up Commands for OHS

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.example.com -port
7777 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.example.com
-port 7778 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name ohs3 -description "ohs3 local
configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
-shared false
```

  - Shared config:

```
topotool.sh add -confighome -name ohs3 -description "ohs3 shared
configuration home" -path " /u02/private/oracle/config/instances/ohs3"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename webhost3.example.com -name ohs3
-description "ohs3" -type OHS_HTTPD -tier WEB -mwhomename Webtier:MW_HOME
-hometype WEBTIER -confighomename ohs3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
ohs3:webhost3,ohs3:webhost3:ssl
```

- Adding the new host to the load balancer mappings
  - Adding to sso load balancer Mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name sso  -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

  - Adding to igdinternal load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name
igdinternal-physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
```

  - Adding to oimadmin load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

- Adding to oamadmin load balancer mapping

```
topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
ohs3:webhost3,ohs3:webhost3:ssl
```

30.4.3.5 Steps for Adding OPMN for Webtier Scale Up and Scale Out

1. Add a non-SSL host if OPMN is listening on non-SSL port.
2. Add a SSL host if OPMN is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
4. Add an instance of type OPMN, tier WEB, hometype WEBTIER using an existing web tier middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.

30.4.3.6 Commands for Adding OPMN Instance for WEB Tier for Scale Out and Scale Up

- Adding new host (hostname + port combination)
  - Non-SSL:

```
topotool.sh add -host -name OPMN:ohs3 -fqdn webhost3.example.com -port 6700
-secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name OPMN:webhost3:ssl -fqdn webhost3.example.com
-port 6701 -secure true -virtual false
```

- Adding new instance

```
topotool.sh add -instance -machinename webhost3.example.com -name OPMN:ohs3
-description "opmn for ohs third instance" -type OPMN -tier WEB -mwhomename
Webtier:MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename OPMN:ohs3 -type DEFAULT -hosts
OPMN:webhost3, OPMN:webhost3:ssl
```

31

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the Identity and Access Management topology. These operations include monitoring, scaling, backing up your topology, and troubleshooting.

This chapter includes the following topics:

31.1 Starting and Stopping Enterprise Deployment Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment.

This section contains the following topics:

31.1.1 Startup and Shutdown Order

When starting up your entire infrastructure, start the components in the following order, (ignoring those not in your topology):

1. Database(s)
2. Database Listener(s)
3. Web hosts
4. LDAP hosts
5. OAM hosts
6. OIM hosts
7. Oracle Identity Manager Administration Server
8. Oracle Identity Manager Managed Servers
9. Oracle Access Management Administration Server
10. Oracle Access Management Managed Servers
11. Oracle Web Servers
12. Oracle Mobile Security Access Servers

Note: To shutdown the servers, follow the reverse order.

31.1.2 Stopping and Starting Exalogic vServers

This section describes how to stop and start Exalogic vServers.

This section contains the following topics

- Section 31.1.2.1, "Stopping vServers"
- Section 31.1.2.2, "Starting vServers"

31.1.2.1 Stopping vServers

To stop a vServer, do the following:

Note: Do not use the `xm destroy` command or Oracle VM Manager to stop a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Under vDCs, expand your cloud such as `MyCloud`.
4. Expand **Accounts**.
5. Expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.
6. Select the **vServer** you wish to stop.

   The dashboard of the vServer is displayed.
7. From the actions pane on the right, click **Stop vServer**. Wait till the job succeeds in the jobs pane.

31.1.2.2 Starting vServers

To start a vServer, do the following:

> **Note:** Do not use the `xm create` command or Oracle VM Manager to start a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Expand your cloud, such as `MyCloud`.
4. Expand **Accounts**.
5. Expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.
6. Select the **vServer** you wish to start.

   The dashboard of the vServer is displayed.
7. From the actions pane on the right, click **Start vServer**. Wait till the job succeeds in the jobs pane.

31.1.3 Starting and Stopping Directory Services

This section describes how to start and stop the directory services. This section includes the following topics:

- Section 31.1.3.1, "Starting and Stopping Oracle Unified Directory"
- Section 31.1.3.2, "Starting and Stopping Oracle Internet Directory"
- Section 31.1.3.3, "Starting and Stopping Oracle Active Directory"

31.1.3.1 Starting and Stopping Oracle Unified Directory

This section describes how to start and stop Oracle Unified Directory.

This section includes the following topics:

- Section 31.1.3.1.1, "Starting Oracle Unified Directory"
- Section 31.1.3.1.2, "Stopping Oracle Unified Directory"

31.1.3.1.1 Starting Oracle Unified Directory To start Oracle Unified Directory, run the following command:

```
LDAP_ORACLE_INSTANCE/OUD/bin/start-ds
```

31.1.3.1.2 Stopping Oracle Unified Directory To stop Oracle Unified Directory, run the command:

```
LDAP_ORACLE_INSTANCE/OUD/bin/stop-ds
```

31.1.3.2 Starting and Stopping Oracle Internet Directory

This section describes how to start and stop Oracle Internet Directory.

This section includes the following topics:

- Section 31.1.3.2.1, "Starting Oracle Internet Directory"
- Section 31.1.3.2.2, "Stopping Oracle Internet Directory"

31.1.3.2.1 Starting Oracle Internet Directory To start Oracle Internet Directory, run the following command:

```
OID_ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started, using the following command:

```
OID_ORACLE_INSTANCE/bin/opmnctl status -l
```

31.1.3.2.2 Stopping Oracle Internet Directory To stop Oracle Internet Directory, run the following command:

```
OID_ORACLE_INSTANCE/bin/opmnctl stopall
```

31.1.3.3 Starting and Stopping Oracle Active Directory

Refer to the Oracle Active Directory documentation for instructions on starting and stopping Oracle Active Directory.

31.1.4 Starting and Stopping Node Manager

This section described how to start and stop the Node Manager.

This section includes the following topics:

- Section 31.1.4.1, "Starting Node Manager"
- Section 31.1.4.2, "Stopping Node Manager"

31.1.4.1 Starting Node Manager

If the Node Manager being started is the one that controls the Administration Server, then prior to starting the Node Manager, run the command:

```
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
```

To start the Node Manager, run the following command:

```
cd SHARED_CONFIG_DIR/nodemanager/hostname
./startNodeManagerWrapper.sh
```

31.1.4.2 Stopping Node Manager

To stop the Node Manager, kill the process started in the previous section.

31.1.5 Starting and Stopping IAMAccessDomain Services

This section descries how to start and stop IAMAccessDomain services.

This section contains the following topics:

- Section 31.1.5.1, "Starting and Stopping a WebLogic Administration Server"
- Section 31.1.5.2, "Starting and Stopping Oracle Access Manager Weblogic Managed Servers"

- Section 31.1.5.3, "Starting and Stopping Policy Manager Weblogic Managed Servers"
- Section 31.1.5.4, "Starting and Stopping Mobile Security Manager Weblogic Managed Servers"

31.1.5.1 Starting and Stopping a WebLogic Administration Server

This section describes how to start and stop a WebLogic Administration Server.

This section includes the following topics:

- Section 31.1.5.1.1, "Starting a WebLogic Administration Server"
- Section 31.1.5.1.2, "Stopping a WebLogic Administration Server"

Notes:

- *Admin_User* and *Admin_Password* are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the file: *IAD_ASERVER_HOME*/config/nodemanager/nm_password.properties
- If you are starting the IAMAccessDomain Administration server, *ASERVER_HOME* is *IAD_ASERVER_HOME*. If you are starting the IAMGovernanceDomain Administration server, *ASERVER_HOME* is *IGD_ASERVER_HOME*

31.1.5.1.1 Starting a WebLogic Administration Server The recommended way to start the Administration server is to use WLST and connect to Node Manager:

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

Where *ORACLE_COMMON_HOME* is from the *MW_HOME* associated with the domain you are starting or stopping.

To start the Administration Server in the Access Domain, use the following command:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','IAD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain')
nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
ASERVER_HOME/bin/startWebLogic.sh
```

Note: The Node Manager admin password is the *COMMON_IAM_PASSWORD*.

31.1.5.1.2 Stopping a WebLogic Administration Server To stop the Administration Server, log in to the WebLogic console using the URL listed in Section 31.2, "About Identity

and Access Management Console URLs"

Then proceed as follows:

1. Click the **Control** tab.
2. Select **AdminServer(admin)**.
3. Click **Shutdown** and select **Force Shutdown now**.
4. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

31.1.5.2 Starting and Stopping Oracle Access Manager Weblogic Managed Servers

This section describes how to start and stop the Oracle Access Manager Managed Servers.

This section includes the following topics:

- Section 31.1.5.2.1, "Starting Oracle Access Manager WebLogic Managed Servers"
- Section 31.1.5.2.2, "Stopping Oracle Access Manager WebLogic Managed Servers"

31.1.5.2.1 Starting Oracle Access Manager WebLogic Managed Servers To start a Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select the Oracle Access Manager Managed Server. For example, **wls_oam1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.5.2.2 Stopping Oracle Access Manager WebLogic Managed Servers To stop a Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select the Oracle Access Manager Managed Server. For example, **wls_oam1**.
4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.5.3 Starting and Stopping Policy Manager Weblogic Managed Servers

This section describes how to start and stop Policy Manager Managed Servers.

This section includes the following topics:

- Section 31.1.5.3.1, "Starting Policy Manager WebLogic Managed Servers"
- Section 31.1.5.3.1, "Starting Policy Manager WebLogic Managed Servers"

31.1.5.3.1 Starting Policy Manager WebLogic Managed Servers To start a Policy Manager Managed Server(s), log in to the WebLogic console using the URL listed in

Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select the Policy Manager Managed Server. For example, **wls_ama1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.5.3.2 Stopping Policy Manager WebLogic Managed Servers To stop a Policy Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select the Policy Manager Managed Server. For example, **wls_ama1**.
4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.5.4 Starting and Stopping Mobile Security Manager Weblogic Managed Servers

This section describes how to start and stop Oracle Mobile Security Manager Managed Servers.

This section includes the following topics:

- Section 31.1.5.4.1, "Starting Mobile Security Manager WebLogic Managed Servers"
- Section 31.1.5.4.2, "Stopping Mobile Security Manager WebLogic Managed Servers"

31.1.5.4.1 Starting Mobile Security Manager WebLogic Managed Servers To start a Mobile Security Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select the Mobile Security Manager Managed Server. For example, **wls_msm1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.5.4.2 Stopping Mobile Security Manager WebLogic Managed Servers To stop a Mobile Security Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.

3. Select the Mobile Security Manager Managed Server. For example, **wls_msm1**.
4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.6 Starting and Stopping IAMGovernanceDomain Services

This section descries how to start and stop IAMGovernanceDomain services.

This section contains the following topics:

- Section 31.1.6.1, "Starting and Stopping a WebLogic Administration Server"
- Section 31.1.6.2, "Starting and Stopping Oracle SOA Suite Weblogic Managed Servers"
- Section 31.1.6.3, "Starting and Stopping Oracle Identity Manager Weblogic Managed Servers"
- Section 31.1.6.4, "Starting and Stopping Oracle BI Publisher Weblogic Managed Servers"

31.1.6.1 Starting and Stopping a WebLogic Administration Server

This section describes how to start and stop a WebLogic Administration Server.

This section includes the following topics:

- Section 31.1.6.1.1, "Starting a WebLogic Administration Server"
- Section 31.1.6.1.2, "Stopping a WebLogic Administration Server"

Notes:

- *Admin_User* and *Admin_Password* are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the file: *IAD_ASERVER_HOME*/config/nodemanager/nm_password.properties
- If you are starting the IAMAccessDomain Administration server, *ASERVER_HOME* is *IAD_ASERVER_HOME*. If you are starting the IAMGovernanceDomain Administration server, *ASERVER_HOME* is *IGD_ASERVER_HOME*

31.1.6.1.1 Starting a WebLogic Administration Server The recommended way to start the Administration server is to use WLST and connect to Node Manager:

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

Where *ORACLE_COMMON_HOME* is from the *MW_HOME* associated with the domain you are starting or stopping.

To start the Administration Server in the IAMGovernanceDomain, use the following command:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMGovernanceDomain','IAD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMGovernanceDomain','/u01/oracle/config/domains/IAMGovernanceDomain')
nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
ASERVER_HOME/bin/startWebLogic.sh
```

> **Note:** The Node Manager admin password is the *COMMON_IAM_PASSWORD*.

31.1.6.1.2 Stopping a WebLogic Administration Server To stop the Administration Server, log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs"

Then proceed as follows:

1. Click the **Control** tab.
2. Select **AdminServer(admin)**.
3. Click **Shutdown** and select **Force Shutdown now**.
4. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

31.1.6.2 Starting and Stopping Oracle SOA Suite Weblogic Managed Servers

This section describes how to start and stop the Oracle SOA Suite Managed Servers.

This section includes the following topics:

- Section 31.1.6.2.1, "Starting Oracle SOA Suite WebLogic Managed Servers"
- Section 31.1.6.2.2, "Stopping Oracle SOA Suite WebLogic Managed Servers"

31.1.6.2.1 Starting Oracle SOA Suite WebLogic Managed Servers To start a Oracle SOA Suite Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select the Oracle SOA Suite Managed Server. For example, **wls_soa1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.6.2.2 Stopping Oracle SOA Suite WebLogic Managed Servers To stop a Oracle SOA Suite Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select the Oracle SOA Suite Managed Server. For example, **wls_soa1**.

4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.6.3 Starting and Stopping Oracle Identity Manager Weblogic Managed Servers

This section describes how to start and stop Oracle Identity Manager Managed Servers.

This section includes the following topics:

- Section 31.1.6.3.1, "Starting Oracle Identity Manager WebLogic Managed Servers"
- Section 31.1.6.3.2, "Stopping Oracle Identity Manager WebLogic Managed Servers"

31.1.6.3.1 Starting Oracle Identity Manager WebLogic Managed Servers To start a Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select the Oracle Identity Manager Managed Server. For example, **wls_oim1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.6.3.2 Stopping Oracle Identity Manager WebLogic Managed Servers To stop a Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select the Oracle Identity Manager Managed Server. For example, **wls_oim1**.
4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.6.4 Starting and Stopping Oracle BI Publisher Weblogic Managed Servers

This section describes how to start and stop Oracle BI Publisher Managed Servers.

This section includes the following topics:

- Section 31.1.5.4.1, "Starting Mobile Security Manager WebLogic Managed Servers"
- Section 31.1.5.4.2, "Stopping Mobile Security Manager WebLogic Managed Servers"

31.1.6.4.1 Starting Oracle BI Publisher WebLogic Managed Servers To start a Oracle BI Publisher Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.

3. Select the Oracle BI Publisher Managed Server. For example, **wls_bi1**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

31.1.6.4.2 Stopping Oracle BI Publisher WebLogic Managed Servers To stop Oracle BI Publisher Managed Server(s), log in to the WebLogic console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs".

Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select the Oracle BI Publisher Managed Server. For example, **wls_bi1**.
4. Click **Shutdown** and then click **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

31.1.7 Starting and Stopping Web Servers

This section describes how to start and stop web services like Oracle HTTP Server, Oracle Traffic Director, and Oracle Mobile Access Server.

This section includes the following topics:

- Section 31.1.7.1, "Starting and Stopping Oracle HTTP Server"
- Section 31.1.7.2, "Starting the Oracle Traffic Director Instances"
- Section 31.1.7.3, "Starting and Stopping Oracle Mobile Access Server"

31.1.7.1 Starting and Stopping Oracle HTTP Server

This section describes how to start and stop Oracle HTTP Server.

Prior to starting/stopping the Oracle HTTP server ensure that the environment variables *WEB_ORACLE_HOME* and *ORACLE_INSTANCE* are defined and that *ORACLE_HOME*/opmn/bin appears in the *PATH*. For example:

```
export ORACLE_HOME=WEB_ORACLE_HOME
export ORACLE_INSTANCE=WEB_ORACLE_INSTANCE
export PATH=$ORACLE_HOME/opmn/bin:$PATH
```

This section includes the following topics:

- Section 31.1.7.1.1, "Starting Oracle HTTP Server"
- Section 31.1.7.1.2, "Stopping Oracle HTTP Server"

31.1.7.1.1 Starting Oracle HTTP Server To start the Oracle HTTP Server, run the following command:

```
opmnctl startall
```

31.1.7.1.2 Stopping Oracle HTTP Server To stop the Oracle HTTP Server, run the following command:

To stop the entire Web tier:

```
opmnctl stopall
```

To stop Oracle HTTP Server only:

```
opmnctl stoproc process-type=OHS
```

31.1.7.2 Starting the Oracle Traffic Director Instances

To start Oracle Traffic Director instances using the administration console, do the following

1. Log in to the administration console using the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. Click **Configurations** at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to start the instance.
4. In the navigation pane, select **Instances**.
5. Click **Start/Restart** for the instance that you want to start.

This section also includes the following topics:

- Section 31.1.7.2.1, "Starting and Stopping Oracle Traffic Director Administration Instances"
- Section 31.1.7.2.2, "Starting Oracle Traffic Director Instances"
- Section 31.1.7.2.3, "Starting Oracle Traffic Director Failover groups"

31.1.7.2.1 Starting and Stopping Oracle Traffic Director Administration Instances OTD administration instances must be running to enable access to the OTD administration console and to enable the administration console to control remote OTD instances. To start the OTD administration console: perform the following steps.

Execute the command `startserv` located in the directory: *WEB_ORACLE_INSTANCE*`/admin-server/bin`

To stop the Administration Services, execute the command `stopserv` located in the directory: *WEB_ORACLE_INSTANCE*`/admin-server/bin`

Note: If you are not running Oracle Traffic Director as root, manually stop the OTD failover groups first using the following command:

OTD_ORACLE_HOME`/bin/tadm stop-failover --instance-home=`*WEB_INSTANCE_HOME*`/ --config=login.example.com`

31.1.7.2.2 Starting Oracle Traffic Director Instances To start or restart *all* instances of the selected configuration, click **Start/Restart Instances** in the Common Tasks pane. To stop all instances of the configuration, click **Stop Instances**.

31.1.7.2.3 Starting Oracle Traffic Director Failover groups If you started your OTD instances as the software owner rather than `root`, then start OTD failover groups using the following command when you are logged in as `root`:

WEB_ORACLE_HOME`/bin/tadm start-failover --instance-home=`*WEB_INSTANCE_HOME*`/ --config=IAM`

If you did not configure your Oracle Traffic Director to start as root, manually start the failover groups using the following command as root:

OTD_ORACLE_HOME`/bin/tadm start-failover --instance-home=`*WEB_INSTANCE_HOME*`/`

```
--config=login.example.com
```

31.1.7.3 Starting and Stopping Oracle Mobile Access Server

This section describes how to start and stop Oracle Mobile Access Server.

This section includes the following topics:

- Section 31.1.7.3.1, "Starting Oracle Mobile Access Server"
- Section 31.1.7.3.2, "Stopping Oracle Mobile Access Server"

31.1.7.3.1 Starting Oracle Mobile Access Server To start the Oracle Mobile Access Server, run the following command:

MSAS_INSTANCE_HOME/bin/startServer.sh

31.1.7.3.2 Stopping Oracle Mobile Access Server To stop the Oracle Mobile Access Server, run the following command:

MSAS_INSTANCE_HOME/bin/stopServer.sh

31.2 About Identity and Access Management Console URLs

Table 31–1 lists the administration consoles used in this guide and their URLs.

Table 31–1 Console URLs

Domain	Console	URL	Administrator User Name
IAMAccessDomain	WebLogic Administration Console	http://IADADMIN.example.com/console	weblogic_idm
	Enterprise Manager FMW Control	http://IADADMIN.example.com/em	weblogic_idm
	OAM console	http://IADADMIN.example.com/oamconsole	oamadmin
	Access Management Policy Manager	http://IADADMIN.example.com/access	oamadmin
IAMGovernanceDomain	WebLogic Administration Console	http://IGDADMIN.example.com/console	weblogic_idm
	Enterprise Manager FMW Control	http://IGDADMIN.example.com/em	weblogic_idm
	Identity Manager System Administration Console	http://IGDADMIN.example.com/sysadmin	xelsysadm
	Oracle Identity Self Service	https://prov.example.com/identity	xelsysadm

Table 31–1 (Cont.) Console URLs

Domain	Console	URL	Administrator User Name
N/A	Exalogic Control (Enterprise Manager Operations Control)	`https://exalogic:9943/emoc`	
N/A	Oracle Traffic Director Administration Console	`https://OTDADMINVHN.example.com:8989`	`otdadmin`
N/A	Oracle ZFS Storage Appliance Browser User Interface	`https://exalogicsn01-priv:215`	

31.3 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 31.3.1, "Monitoring Oracle Unified Directory"
- Section 31.3.2, "Monitoring WebLogic Managed Servers"

31.3.1 Monitoring Oracle Unified Directory

You can check the status of Oracle Unified Directory by issuing the command:

```
LDAP_ORACLE_INSTANCE/OUD/bin/status
```

This command prompts for the OUD Admin username and *OUD_COMMON_PASSOWORD*.

This command accesses the locally running Oracle Unified Directory instance and reports the status of the directory, including whether or not replication and LDAP or LDAPS is enabled.

31.3.2 Monitoring WebLogic Managed Servers

You can use Oracle Enterprise Manager Fusion Middleware Control to monitor Managed Servers and other Fusion Middleware components, such as Access Manager, Oracle Identity Manager, Oracle Identity Federation, and SOA. For more information, see the administrator guides listed in the Preface under "Related Documents".

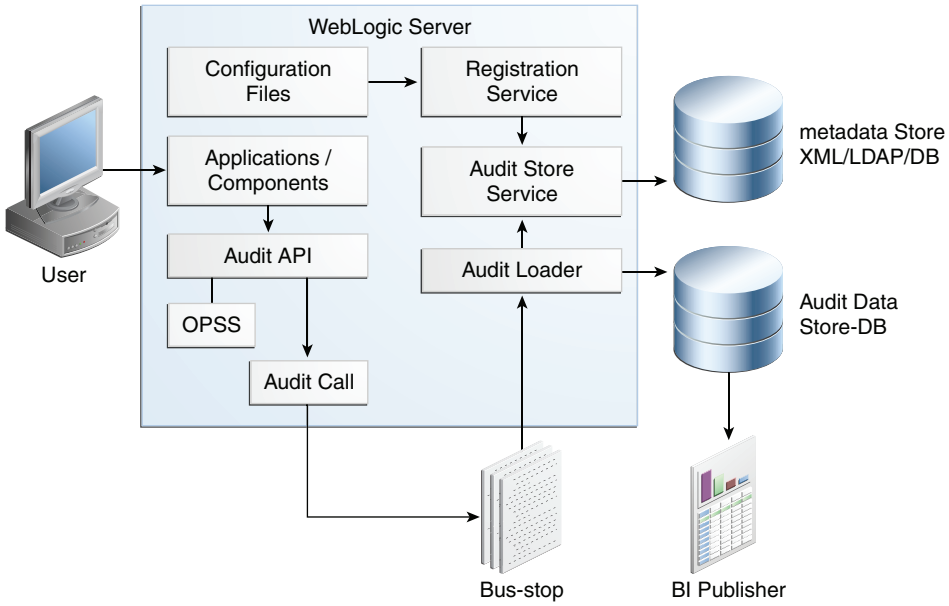
31.4 Auditing Identity and Access Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications are able to create application-specific

audit events. For non-JavaEE Oracle components in the middleware such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

Figure 31–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework. For more information, see *Oracle Fusion Middleware Application Security Guide*.

Figure 31–1 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.

31.5 Performing Backups and Recoveries

You can use the UNIX `tar` command for most backups. Typical usage is:

```
tar -czvpsPf BACKUP_LOCATION/backup_file.tar directories
```

You can use the UNIX `tar` command for recovery. Typical usage is:

```
tar -xzvpsPf BACKUP_LOCATION/backup_file.tar
```

For database backup and recovery, you can use the database utility RMAN. See the *Oracle Database Backup and Recovery Reference* for more information on using this command.

This section contains the following topics:

- Section 31.5.1, "Performing Baseline Backups"
- Section 31.5.2, "Performing Runtime Backups"
- Section 31.5.3, "Performing Backups During Installation and Configuration"

31.5.1 Performing Baseline Backups

Perform baseline backups when building a system and when applying patches that update static artifacts, such as the Oracle binaries.

After performing a baseline backup, also perform a runtime backup.

Table 31–2 Static Artifacts to Back Up in the Identity and Access Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	Oracle RAC database hosts: IADDBHOST1 IADDBHOST2	User Defined	Database
Oracle Directory Binaries	LDAPHOST1 LDAPHOST2	Middleware Home: `DIR_MW_HOME`	Directory Tier
Oracle Access Management Binaries	OAMHOST1 OAMHOST2	Middleware Home: *`IAD_MW_HOME`*	Application Tier
Oracle Identity Governance Binaries	OIMHOST1 OIMHOST2	Middleware Home: *`IGD_MW_HOME`*	Application Tier
Web Tier Binaries	WEBHOST1 WEBHOST2	Middleware Oracle home, *`WEB_ORACLE_HOME`*:	Web Tier
Install-Related Files	Each host	OraInventory: *`ORACLE_BASE`*`/oraInventory` `/etc/oratab`, `/etc/oraInst.loc` `~/bea/beahomelist` (on hosts where WebLogic Server is installed)	Not applicable.

Note: It is also recommended that you back up your load balancer configuration. Refer to your vendor documentation on how to do this.

For more information on backup and recovery of Oracle Fusion Middleware components, refer to the following chapters in the *Oracle Fusion Middleware Administrator's Guide*:

- Introducing Backup and Recovery
- Backing Up Your Environment
- Recovering Your Environment

31.5.2 Performing Runtime Backups

Perform runtime backups on an ongoing basis. These backups contain information on items that can change frequently, such as data in the database, domain configuration information, and identity information in LDAP directories.

Table 31–3 Run-Time Artifacts to Back Up in the Identity and Access Management Enterprise Deployments

Type	Host	Location	Tier
IAMAccessDomain Home	OAMHOST1 OAMHOST2	Administration Server and Shared Files: *IAD_ASERVER_HOME* Managed Servers: *IAD_MSERVER_HOME*	Application Tier
IAMGovernanceDomain Home	OIMHOST1 OIMHOST2	Administration Server and Shared Files: *IGD_ASERVER_HOME* Managed Servers: *IGD_MSERVER_HOME*	Application Tier
Oracle HTTP Server	WEBHOST1 WEBHOST2	*OHS_ORACLE_INSTANCE*	Web Tier
Oracle Traffic Director	WEBHOST1 WEBHOST2	*OTD_ORACLE_INSTANCE*	Web Tier
Mobile Security Access Server	WEBHOST1 WEBHOST2	*MSAS_ORACLE_INSTANCE*	Web Tier
Oracle RAC Databases	IADDBHOST1 IADDBHOST2	User defined	Database
Oracle Unified Directory	LDAPHOST1 LDAPHOST2	*OUD_ORACLE_INSTANCE*	Directory Tier
Oracle Internet Directory	LDAPHOST1 LDAPHOST2	*OID_ORACLE_INSTANCE*	Directory Tier

31.5.3 Performing Backups During Installation and Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process.

For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

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

This section contains the following topics:

- Section 31.5.3.1, "Backing Up Middleware Home"
- Section 31.5.3.2, "Backing Up LDAP Directories"
- Section 31.5.3.3, "Backing Up the Database"
- Section 31.5.3.4, "Backing Up the WebLogic Domain IAMGovernanceDomain"

- Section 31.5.3.5, "Backing Up the WebLogic Domain IAMAccessDomain"
- Section 31.5.3.6, "Backing Up the Web Tier"

31.5.3.1 Backing Up Middleware Home

Back up the Middleware homes whenever you create a new one or add components to it. The Middleware homes used in this guide are Oracle Identity Management and Oracle Identity and Access Management, as listed in Table 31–2.

31.5.3.2 Backing Up LDAP Directories

Whenever you perform an action which updates the data in LDAP, back up the directory contents.

This section contains the following topics:

- Section 31.5.3.2.1, "Backing Up Oracle Unified Directory"
- Section 31.5.3.2.2, "Backing Up Third-Party Directories"

31.5.3.2.1 Backing Up Oracle Unified Directory To backup Oracle Unified Directory, perform the following steps:

1. Shut down the Oracle Unified Directory Instances as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
2. Back up *LDAP_ORACLE_INSTANCE* directories on each host.
3. Restart the Oracle Unified Directory instances as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

31.5.3.2.2 Backing Up Third-Party Directories Refer to your operating system vendor's documentation for information about backing up directories.

31.5.3.3 Backing Up the Database

Whenever you create add a component to the configuration, back up the IADDB database. Perform this backup after or adding components such as Oracle Access Management Access Manager or Oracle Identity Manager.

31.5.3.4 Backing Up the WebLogic Domain IAMGovernanceDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
2. Back up the *IGD_ASERVER_HOME* directory from shared storage.
3. Back up the *IGD_MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

31.5.3.5 Backing Up the WebLogic Domain IAMAccessDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
2. Back up the *IAD_ASERVER_HOME* directory from shared storage.

3. Back up the *IAD_MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

31.5.3.6 Backing Up the Web Tier

To back up the Web Tier, perform these steps:

31.5.3.6.1 Backing Up Oracle HTTP Server Back up Oracle HTTP Server as follows:

1. Shut down the Oracle HTTP Server as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
2. Back up the *WEB_ORACLE_INSTANCE* directory on local storage.
3. Start the Oracle HTTP Server as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

31.6 Patching Enterprise Deployments

It is recommended that you patch enterprise deployments by using the automated patching solution included with the Identity and Access Management Life Cycle Tools.

The process of applying patches can be summarized as follows:

1. Create a patch top. A patch top directory contains patches, classified by each product to which patches apply.
2. Run Patch Manager to generate a patch plan. Based on the deployment topology and patches provided, the Manager creates an optimal plan to apply those patches.
3. Run the Patcher against all hosts which are affected by the plan. You might need to execute the Patcher on a given host multiple times if required by a given plan. As each Patcher invocation completes, it directs you where to run the Patcher next.

When the Patcher runs, it stops and starts server instances as necessary, and ensures that patches are applied in the correct order to satisfy dependencies.

Full details on how to use the IDM Patching Framework can be found in *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*. The Guide also contains instructions for patching the deployment manually if required, using the OPatch tool.

31.7 Preventing Timeouts for SQL

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall so it does not time out these connections. If such a configuration is not possible, set the SQLNET.EXPIRE_TIME=n parameter in the *ORACLE_HOME*/network/admin/sqlnet.ora file on the database server, where n is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

31.8 Manually Failing Over the WebLogic Administration Server

This section discusses how to fail over the Administration Server to a new host after the primary host fails. The example in this section shows how to fail the Access Management Administration Server from OAMHOST1 to OAMHOST2. If you are failing over the Oracle Identity Manager Administration server, substitute the appropriate values for that domain.

This section contains the following topics:

31.8.1 Failing Over the Administration Server to OAMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from OAMHOST1 to OAMHOST2.

Assumptions:

- The Administration Server is configured to listen on `IADADMINVHN.example.com`, and not on `ANY` address.
- The Administration Server is failed over from OAMHOST1 to OAMHOST2, and the two nodes have these IP addresses:
  - OAMHOST1: `100.200.140.165`
  - OAMHOST2: `100.200.140.205`
  - IADADMINVHN: `100.200.140.206`

    This is the Virtual IP address where the Administration Server is running, assigned to *interface*:*index* (for example, eth1:2), available in OAMHOST1 and OAMHOST2.
- The domain directory where the Administration Server is running in OAMHOST1 is on a shared storage and is mounted also from OAMHOST2.

  Note: NM in OAMHOST2 does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on OAMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, Node Manager is fully functional
- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed in OAMHOST2 as described in previous chapters. That is, the same path for *`IAD_ORACLE_HOME`* and *`IAD_MW_HOME`* that exists in OAMHOST1 is available in OAMHOST2.

The following procedure shows how to fail over the Administration Server to a different node, OAMHOST2.

1. Stop the Administration Server on OAMHOST1 as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
2. Migrate the IP address to the second node.

a. Run the following command as root on OAMHOST1 (where *x*:*y* is the current interface used by `IADADMINVHN.example.com`):

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

For example:

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

b. Run the following command on OAMHOST2:

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

For example:

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

Note: Ensure that the netmask and interface to be used match the available network configuration in OAMHOST2.

3. Update routing tables by using `arping` on OAMHOST2, for example:

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

31.8.2 Starting the Administration Server on OAMHOST2

Perform the following steps to start Node Manager on OAMHOST2.

1. On OAMHOST2, mount the Administration Server domain directory if it is not already mounted. For example:

```
mount /u01/oracle
```

2. Start Node Manager by using the following commands:

```
cd WL_HOME/server/bin
./startNodeManager.sh
```

3. Stop the Node Manager by killing the Node Manager process.

Note: Starting and stopping Node Manager at this point is only necessary the first time you run Node Manager. Starting and stopping it creates a property file from a predefined template. The next step adds properties to that property file.

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

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

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

5. Start the Node Manager as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."

6. Start the Administration Server on OAMHOST2.

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

   Once in the WLST shell, execute the following commands:

   ```
   nmConnect('admin','Admin_Password', 'OAMHOST2','5556',
   'IAMAccessDomain','/u1/oracle/config/domains/IAMAccessDomain')
   nmStart('AdminServer')
   ```

7. Test that you can access the Administration Server on OAMHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console at:

      `http://IADADMINVHN.example.com/console.`

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

31.8.3 Validating Access to OAMHOST2 Through Oracle HTTP Server

Check if you can access the Administration Server when it is running on OAMHOST2.

31.8.4 Failing the Administration Server Back to OAMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on OAMHOST2 and run it on OAMHOST1. To do this, migrate IADADMINVHN back to OAMHOST1 node as described in the following steps.

1. Ensure that the Administration Server is not running on OAMHOST2. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from *IAD_ASERVER_HOME*`/bin`.
2. On OAMHOST2, unmount the Administration server domain directory. For example:

   ```
   umount /u01/oracle
   ```

3. On OAMHOST1, mount the Administration server domain directory. For example:

   ```
   mount /u01/oracle
   ```

4. Disable the `IADADMINVHN.example.com` virtual IP address on OAMHOST2 and run the following command as `root` on OAMHOST2:

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

   where *x*:*y* is the current interface used by `IADADMINVHN.example.com`.

5. Run the following command on OAMHOST1:

   ```
   /sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
   ```

   Note: Ensure that the netmask and interface to be used match the available network configuration in OAMHOST1

6. Update routing tables by using arping. Run the following command from OAMHOST1.

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

7. If Node Manager is not already started on OAMHOST1, start it, as described in Section 31.1, "Starting and Stopping Enterprise Deployment Components."
8. Start the Administration Server again on OAMHOST1.

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

   Once in the WLST shell, execute

   ```
   nmConnect(admin,'Admin_Pasword, OAMHOST1,'5556',
        'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain'
   nmStart('AdminServer')
   ```

9. Test that you can access the Oracle WebLogic Server Administration Console at:

   ```
   http://IADADMINVHN.example.com:7001/console
   ```

   where `7001` is *WLS_ADMIN_PORT* in Section 8.1, "Summary of Virtual IP Addresses Required."
10. Check that you can access and verify the status of components in the Oracle Enterprise Manager at:

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

31.9 Changing Startup Location

When the environment was deployed, start and stop scripts were generated to start and stop components in the topology. At the time of Deployment, the Access Domain Administration server was configured to start on OAMHOST1. If you want to permanently change this to start on OAMHOST2, perform the following steps.

Use the same steps, changing the name of the server and host, to change the Governance Domain Administration server to start on OIMHOST2 instead of OIMHOST1.

Edit the file `serverInstancesInfo.txt`, which is located in the directory: *SHARED_CONFIG_DIR*`/scripts`

Locate the line which looks like this:

```
OAMHOST1.example.com AS AdminServer
```

Change `OAMHOST1` to `OAMHOST2` and save the file.

31.10 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 31.10.1, "Troubleshooting Oracle Traffic Director"
- Section 31.10.2, "Troubleshooting Identity and Access Management Deployment When Using IDMLCM"
- Section 31.10.3, "Troubleshooting IDMLCM Start/Stop Scripts"
- Section 31.10.4, "Troubleshooting Oracle Access Management Access Manager 11g"

- Section 31.10.5, "Troubleshooting Oracle Identity Manager"
- Section 31.10.6, "Troubleshooting Oracle SOA Suite"
- Section 31.10.7, "General Troubleshooting"

31.10.1 Troubleshooting Oracle Traffic Director

This section describes possible issues for Oracle Traffic Director (OTD). It contains the following topics:

- Section 31.10.1.1, "OTD Failover Groups Show as Started, but IP Address Cannot be Pinged"
- Section 31.10.1.2, "Error When Accessing SSL Terminated URL"
- Section 31.10.1.3, "Error When Creating Failover Groups"

31.10.1.1 OTD Failover Groups Show as Started, but IP Address Cannot be Pinged

Problem

OTD failover groups show as started, but IP address cannot be pinged.

Failover groups require a distinct Router ID on the system. If you reuse a Router ID, this behavior occurs. This can even occur if you remove and reinstall OTD.

Solution

To resolve this issue, recreate the failover group using a different Router ID

31.10.1.2 Error When Accessing SSL Terminated URL

Problem

When you access an SSL terminated URL, an error that says the browser cannot connect to the server, is displayed.

Solution

To resolve this issue, do the following:

1. Ensure that the WebLogic plugin in enabled in the domain.
2. Ensure that the SSL Passthrough is enabled in OTD.
3. Ensure that the load balancer is adding WL-Proxy-SSL true and IS_SSL ssl to the HTTP request header. Different load balancers do this in different ways. On BigIP, you create an irule with the following content:

```
# Notify the backend servers that this traffic was SSL offloaded by the F5.

##

when HTTP_REQUEST {

HTTP::header insert WL-Proxy-SSL true
HTTP::header insert IS_SSL ssl

}
```

31.10.1.3 Error When Creating Failover Groups

Problem

When creating failover groups, the following error is seen:

```
OTD-67322 The specified virtual IP 'x.x.x.x' cannot be bound to any of the network
interfaces on the node 'hostname'. The IP addresses bound to the node are [......]
check if the specified virtual IP is in the proper subnet. This error could also
be caused if either the network interfaces on the node are not configured
correctly or if the network prefix length is incorrect.
```

Solution

This is due to the IP address or CIDR being incompatible with the IP address or subnet already configured on the network card you wish to bind to. Choose a different IP address or CIDR.

31.10.2 Troubleshooting Identity and Access Management Deployment When Using IDMLCM

This section describes some common problems related to Deployment. It contains the following topics:

- Section 31.10.2.1, "Deployment Fails"
- Section 31.10.2.2, "Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute"
- Section 31.10.2.3, "Connection to Directory Failed Exception"
- Section 31.10.2.4, "Deployment Fails on Install Phase with Permission Denied Error"
- Section 31.10.2.5, "Deployment Fails While Configuring MSAS"
- Section 31.10.2.6, "Deployment Fails with Error: DiskSpaceCheck SEVERE Disk space check has failed"
- Section 31.10.2.7, "Preverify Inappropriately Fails with Insufficient Space"
- Section 31.10.2.8, "General Troubleshooting"

31.10.2.1 Deployment Fails

Problem

Deployment fails.

Solution

Check the Deployment logs located in the directory:

LCM_HOME/provisioning/logs/*hostname*

where *hostname* is the host where the Deployment step failed.

Rectify the error and re-deploy.

31.10.2.2 Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute

Problem

Deployment fails with an error similar to this:

```
Incorrect host format for attibute : PRIMARY_OAM_SERVERS : server-123.example.com
```

Due to a bug, one of the tools invoked during the deployment process cannot handle host names or domain names containing the hyphen (-) character.

Solution

Use host names and domain names that do NOT contain the hyphen (-) character.

31.10.2.3 Connection to Directory Failed Exception

Problem

You see the following error in the log configure log file:

```
oracle.idm.automation.exception.ExecutionFailedException: Connection to Directory
failed: Host/Port details incorrect
```

Solution

1. Check the property file mentioned in the log file output.

   A line similar to the following appears a bit farther in the log:

   ```
   See [/u01/oracle/products/products/access/iam/idmtools/bin/idmConfigTool.sh,
   -configOAM, input_
   file=/u01/lcm/tools/idmlcm/provisioning/idm-provisioning-build/config/config_
   oam.properties, log_
   file=/u01/lcm/provisioning/logs/slcn04cn10.example.com/idmautomation-configOAM.
   log, log_level=FINEST]{3}
   ```

   From this output you can see that the property file is called `config_oam.properties`. This file however, is moved from the location stated to the log directory. Examine this file and check that the entries `IDSTORE_HOST/IDSTORE_PORT` reference your load balancer/OTD directory entry (`LBR_LDAP_HOST/LBR_LDAP_PORT`).

2. Validate that you can connect to the directory on the local host by telnetting to the LDAP_HOST and LDAP_PORT for example.

   ```
   telnet ldaphost1 1389
   ```

   If you see an entry similar to:

   ```
   Trying 10.245.169.148...
        Connected to slcn04cn10.example.com (10.245.169.148).
        Escape character is '^]'.
   ```

   Then you know that the directory was configured and is running.

   If it is not, the directory was not successfully configured, Check the standard directory log files for more information.

3. Check that you can connect to the directory using the load balancer or OTD entry using `LBR_LDAP_HOST` and `LBR_LDAP_PORT` for example:

   ```
   telnet idstore.example.com 389
   ```

   If you don't see a connection, your load balancer or OTD instance is incorrectly configured. Recheck the configuration.

31.10.2.4 Deployment Fails on Install Phase with Permission Denied Error

Problem

During the Install phase, you may see an error similar to the following in the deployment log file:

```
[runIAMDeployment-install] [NOTIFICATION] []
[runIAMDeployment-install] [tid: 140] [ecid: 0000L3D9WwL72Fk5Gzl3if1ME9aO000013,0]
java.util.concurrent.ExecutionException: java.lang.RuntimeException:
oracle.idm.util.command.CommandException: Invalid shell command.[[
Message: cp: cannot create regular file
`/u01/lcm/lcmconfig/patch/patches/1446550807380/oam/21544485/etc/xml/GenericAction
s.xml: Permission denied
cp: cannot create regular file
`/u01/lcm/lcmconfig/patch/patches/1446550807380/oam/21544485/etc/xml/ShiphomeDirec
toryStructure.xml: Permission denied
```

Solution

This occurs if the patch files have incorrect permissions. When you added patches to your repository, the patch files might not have write permissions which cause the patch manager process to fail.

To resolve the issue, change the permissions of the patch files in the repository to include write permission. For example:

```
chmod -R 755 REPOS_HOME/installers/iamsuite/patch
```

31.10.2.5 Deployment Fails While Configuring MSAS

Problem

The deployment fails in the Preconfig stage of the OAMHOST. The following error message is displayed in the *LCM_HOME*/provisioning/logs/*oamhost1.example.com*/configMSAS.log file:

```
 [wsm] [ERROR] [WSM-02381]
 [oracle.wsm.resources.policymanager] [host: slc00drb] [nwaddr: 10.242.27.183]
[tid: 1] [userId:
user1] [ecid: 0000L4HZ^u717iK5IVG7yf1MIY1L000001,0] Unable to invoke method "post"
of class
com.sun.jersey.api.client.WebResource$Builder" with values
"[Ljava.lang.Object;@497275cd"
```

Solution

This is caused by the IAD callback entry point being incorrectly configured. Ensure that `iadinternal.example.com:port` is correctly configured as described in Chapter 6, "Preparing the Load Balancer and Firewalls for an Enterprise Deployment".

31.10.2.6 Deployment Fails with Error: DiskSpaceCheck SEVERE Disk space check has failed

Problem

The IDMLCM tool health check verifies the disk space at *IDM_TOP* and fails, even though all the mounted storage shares under IDM_TOP have sufficient storage space, hence causing the deployment to fail.

Solution

The workaround for this issue is as follows:

1. Look for the plugin definition with name "DiskSpaceCheck" in the *IDMLCM_HOME*/healthcheck/config/PreInstallChecks_mandatory.xml file, and comment out the plugin definition.
2. Run the deployment again.

31.10.2.7 Preverify Inappropriately Fails with Insufficient Space

Problem

When preverify runs, it checks that sufficient space is available in the directory *IDM_TOP*. If you have created separate mount points for *IDM_TOP*/products and *IDM_TOP*/config, preverify does not add together the space allocated to the two mount points and fails the check inappropriately.

Solution

Disable the free space check by editing the file:

LCM_HOME/provisioning/idm-provisioning-build/idm-common-preverify-build.xml

Locate the entry:

```
<target name="common-preverify-tasks">
```

Comment out the following entry so that after editing it looks like this:

```
<!--antcall target="private-preverify-free-space"/-->
```

Save the file.

31.10.2.8 General Troubleshooting

Examine the log files in the directory *LCM_HOME*/provisioning/hostname. For example:

LCM_HOME/provisioning/*hostname*/runIAMDeployment-*stage*.log

This process identifies the cause of the failure.

If Pre-verify fails

If the pre-verify fails check this additional log file:

LCM_HOME/provisioning/*hostname*/healthchecker-preverify-error-check.log

31.10.3 Troubleshooting IDMLCM Start/Stop Scripts

This section describes some common problems related to Start/Stop scripts. It contains the following topics:

- Section 31.10.3.1, "Start/Stop Scripts Fail to Start or Stop a Managed Server"

31.10.3.1 Start/Stop Scripts Fail to Start or Stop a Managed Server

Problem

Problem: Start/Stop scripts fail to start or stop a managed server.

The start/stop logs in the directory *SHARED_CONFIG_DIR*/scripts/logs contain an error similar to this:

```
weblogic.utils.AssertionError: ***** ASSERTION FAILED *****
        at
weblogic.server.ServerLifeCycleRuntime.getStateRemote(ServerLifeCycleRuntime.java:
734)
        at
weblogic.server.ServerLifeCycleRuntime.getState(ServerLifeCycleRuntime.java:581)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

Solution

1. Shut down the failing managed server. You might have to kill the process.
2. Back up the managed server's LDAP data, then remove it. For example:

   ```
   rm -rf LOCAL_CONFIG_DIR/domains/IAMAccessDomain/servers/server_name/data/ldap
   ```

   where *server_name* is the name of the failing managed server.
3. Restart the managed server.

31.10.4 Troubleshooting Oracle Access Management Access Manager 11*g*

This section describes some common problems that can arise with Access Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 31.10.4.1, "Access Manager Runs out of Memory"
- Section 31.10.4.2, "User Reaches the Maximum Allowed Number of Sessions"
- Section 31.10.4.3, "Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed"
- Section 31.10.4.4, "You Are Not Prompted for Credentials After Accessing a Protected Resource"
- Section 31.10.4.5, "Cannot Log In to Access Management Console"
- Section 31.10.4.6, "Oracle Coherence Cluster Startup Errors in WLS_AMA Server Logs"
- Section 31.10.4.7, "Errors in log File when Starting OAM Servers"

31.10.4.1 Access Manager Runs out of Memory

Problem

After Access Manager has been running for a while, you see the following error message in the output:

```
Attempting to allocate 1G bytes
There is insufficient native memory for the Java Runtime Environment to continue.
```

Possible reasons:

- The system is out of physical RAM or swap space.
- In 32 bit mode, the process size limit was reached.

Solutions

- Reduce memory load on the system.
- Increase physical memory or swap space.
- Check if swap backing store is full.
- Use 64 bit Java on a 64 bit OS.
- Decrease Java heap size (-Xmx/-Xms).
- Decrease number of Java threads.
- Decrease Java thread stack sizes (-Xss).
- Disable compressed references (-XXcompressedRefs=false).
- Ensure that command line tool `adrci` can be executed from the command line.
  - at oracle.dfw.impl.incident.ADRHelper.invoke(ADRHelper.java:1309)

  - at oracle.dfw.impl.incident.ADRHelper.createIncident(ADRHelper.java:929
  - at oracle.dfw.impl.incident.DiagnosticsDataExtractorImpl.createADRIncident(DiagnosticsDataExtractorImpl.java:1116)

- On both OAMHOST1 and OAMHOST2, edit the file `setSOADomainEnv.sh`, which is located in *`IAD_MSERVER_HOME`*`/bin` and locate the line which begins:

  ```
  PORT_MEM_ARGS=
  ```

  Change this line so that it reads:

  ```
  PORT_MEM_ARGS="-Xms768m -Xmx2560m"
  ```

31.10.4.2 User Reaches the Maximum Allowed Number of Sessions

Problem

The Access Manager server displays an error message similar to this:

```
The user has already reached the maximum allowed number of sessions. Please close
one of the existing sessions before trying to login again.
```

Solution

If users log in multiple times without logging out, they might overshoot the maximum number of configured sessions. You can modify the maximum number of configured sessions by using the Access Management Administration Console.

To modify the configuration by using the Access Management Administration Console, proceed as follows:

1. Go to **System Configuration** -> **Common Settings** -> **Session**
2. Increase the value in the **Maximum Number of Sessions per User** field to cover all concurrent login sessions expected for any user. The range of values for this field is from 1 to any number.

31.10.4.3 Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed

Problem

The Administration Server takes a long time to start after configuring Access Manager.

Solution

Tune the Access Manager database. When the Administration server first starts after configuring Access Manager, it creates a number of default policies in the database. If the database is distant or in need of tuning, this can take a significant amount of time.

```
Resources
Authentication Policies
   Protected Higher Level Policy
   Protected Lower Level Policy
   Publicl Policy
Authorization Policies
   Authorization Policies
```

If you do not see these items, the initial population has failed. Check the Administration Server log file for details.

31.10.4.4 You Are Not Prompted for Credentials After Accessing a Protected Resource

Problem

When you access a protected resource, Access Manager should prompt you for your user name and password. For example, after creating a simple HTML page and adding it as a resource, you should see credential entry screen.

Solution

If you do not see the credential entry screen, perform the following steps:

1. Verify that Host Aliases for IAMAccessDomain have been set. You should have aliases for `IAMAccessDomain`:80, `IAMAccessDomain`:Null, `IADADMIN.example.com:80`, and `login.example.com:443`, where Port `80` is *`HTTP_PORT`* and Port `443` is *`HTTP_SSL_PORT`*.
2. Verify that WebGate is installed.
3. Verify that `ObAccessClient.xml` was copied from *`IAD_ASERVER_HOME`*`/output` to the WebGate Lib directory and that OHS was restarted.
4. When `ObAccessClient.xml` was first created, the file was not formatted. When the OHS is restarted, reexamine the file to ensure that it is now formatted. OHS gets a new version of the file from Access Manager when it first starts.
5. Shut down the Access Manager servers and try to access the protected resource. You should see an error saying Access Manager servers are not available. If you do not see this error, re-install WebGate.

31.10.4.5 Cannot Log In to Access Management Console

Problem

You cannot log in to the Access Management Console. The Administration Server diagnostic log might contain an error message similar to this:

```
Caused by: oracle.security.idm.OperationFailureException:
oracle.security.am.common.jndi.ldap.PoolingException [Root exception is
oracle.ucp.UniversalConnectionPoolException:
Invalid life cycle state.
 Check the status of the Universal Connection Pool]
        at
oracle.security.idm.providers.stdldap.UCPool.acquireConnection(UCPool.java:112)
```

Solution

Remove the /tmp/UCP* files and restart the Administration Server.

31.10.4.6 Oracle Coherence Cluster Startup Errors in WLS_AMA Server Logs

Problem

The WLS_AMA2 server has oam application deployment in failed state. The WLS_AMA2 server logs report request timeout exceptions while starting the cluster service, similar to following logs:

```
Oracle Coherence GE 3.7.1.13 <Warning> (thread=Cluster, member=n/a): Delaying
formation of a new cluster; IpMonitor failed to verify the reachability of senior
Member(Id=1, Timestamp=, Address=, MachineId=,
Location=site:,machine:iadadminvhn,process:8499, Role=WeblogicServer); if this
persists it is likely the result of a local or remote firewall rule blocking
either ICMP pings, or connections to TCP port 7>
```

```
Error while starting cluster: com.tangosol.net.RequestTimeoutException: Timeout
during service start: ServiceInfo(Id=0, Name=Cluster, Type=Cluster
MemberSet=MasterMemberSet(
ThisMember=null
OldestMember=null
ActualMemberSet=MemberSet(Size=0
)
MemberId|ServiceVersion|ServiceJoined|MemberState
RecycleMillis=1200000
RecycleSet=MemberSet(Size=0
)
)
)
at
com.tangosol.coherence.component.util.daemon.queueProcessor.service.Grid.onStartup
Timeout(Grid.CDB:3)

at
com.tangosol.coherence.component.util.daemon.queueProcessor.Service.start(Service.
CDB:28)

at
com.tangosol.coherence.component.util.daemon.queueProcessor.service.Grid.start(Gri
d.CDB:6)
```

Solution

This is a known issue. In some of the environments, the Access Policy Manager Server that is not running on the same host as the WebLogic Administration Server is unable to start the coherence cluster service, which results in the oam application deployment to be in failed state. To solve this issue, you must create a server instance for the effected Access Policy Manager Server by completing the following steps:

1. Log in to the OAM console using the following URL:

   `http://`*`iadadmin.example.com`*`/oamconsole`

   Log in as the Access Manager administration user you created when you prepared the ID Store. For example, `oamadmin`.

2. Click **Configuration**.

3. Click **Server Instances** from the configuration launch pad.

4. Click a new server instance for the Access Policy Manager WebLogic Managed Server, that is not running on the same machine as the IAMAccessDomain Admin Server. For example:

   - Name: WLS_AMA2
   - Port: 14150
   - Host: OAMHOST2 (For consolidated topology, the host will be IAMHOST2)

   Note: Provide the OAM Proxy details similar to the server instance for WLS_OAM.

5. Click **Apply**.

31.10.4.7 Errors in log File when Starting OAM Servers

Problem

When you start the OAM Servers, errors similar to the following are seen in the log files which causes LCM heath check module to fail:

```
[wls_oam1] [TRACE:16] [] [oracle.oam.config] [tid: DistributedCacheWorker:4]
[userId: <anonymous>] [ecid:
0000LGmRJqxB9DE5N7P5ie1N5mOd000004,1:16514] [APP: oam_server#11.1.2.0.0] [SRC_
CLASS: oracle.security.am.admin.config.util.MapUtil] [SRC_METHOD:
getDefaultedStringValue] property not found at path:[Ljava.lang.String;@43537067
Defaulting to value:,
[2016-04-20T06:55:39.982+00:00] [wls_oam1] [TRACE:16] [] [oracle.oam.config] [tid:
DistributedCacheWorker:4] [userId: <anonymous>] [ecid:
0000LGmRJqxB9DE5N7P5ie1N5mOd000004,1:16514] [APP: oam_server#11.1.2.0.0] [SRC_
CLASS: oracle.security.am.admin.config.util.MapUtil] [SRC_METHOD: getStringValue]
THROW[[
oracle.security.am.admin.config.ConfigurationException: Cannot get
java.lang.String value from configuration for key ResponseEscapeChar. Object null
found.
at
oracle.security.am.admin.config.util.MapUtil.handleFailedAttributeAccess(MapUtil.j
ava:447)
at oracle.security.am.admin.config.util.MapUtil.getStringValue(MapUtil.java:130)
at
oracle.security.am.admin.config.util.MapUtil.getDefaultedStringValue(MapUtil.java:
147)
at
oracle.security.am.engines.common.identity.provider.util.IdStoreConfig.initializeC
onfig(IdStoreConfig.java:76)
at
oracle.security.am.engines.common.identity.provider.util.IdStoreConfig.<init>(IdSt
oreConfig.java:69)
at
oracle.security.am.engines.common.identity.provider.util.IdStoreConfig.getConfig(I
dStoreConfig.java:128)
at
oracle.security.am.engines.common.identity.util.OAMUserAttribute.getStringValue(OA
MUserAttribute.java:76)
at
oracle.security.am.engines.common.identity.util.OAMUserAttribute.toString(OAMUserA
ttribute.java:114)
at java.lang.String.valueOf(String.java:2849)
at java.lang.StringBuilder.append(StringBuilder.java:128)
at java.util.AbstractMap.toString(AbstractMap.java:523)
at java.lang.String.valueOf(String.java:2849)
at java.lang.StringBuilder.append(StringBuilder.java:128)
at
oracle.security.am.engines.common.identity.util.OAMIdentity.toString(OAMIdentity.j
ava:678)
at java.lang.String.valueOf(String.java:2849)
at java.lang.StringBuilder.append(StringBuilder.java:128)
at oracle.security.am.engines.sso.SSOSubject.toString(SSOSubject.java:238)
at java.lang.String.valueOf(String.java:2849)
at java.lang.StringBuilder.append(StringBuilder.java:128)
at oracle.security.am.engines.sme.impl.SessionImpl.toString(SessionImpl.java:629)
at java.lang.String.valueOf(String.java:2849)
at java.lang.StringBuilder.append(StringBuilder.java:128)
at
oracle.security.am.engines.sme.mapimpl.db.DbOraSmeStore.loadSession(DbOraSmeStore.
```

```
java:1705)
at
oracle.security.am.engines.sme.mapimpl.db.DbOraSmeStore.loadSession(DbOraSmeStore.
java:1691)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
43)
at java.lang.reflect.Method.invoke(Method.java:606)
at
oracle.security.am.foundation.mapimpl.coherence.store.DataConnectionUtility.invoke
SqlOperationWithRetries(DataConnectionUtility.java:275)
at
oracle.security.am.engines.sme.mapimpl.db.DbOraSmeStore.load(DbOraSmeStore.java:12
84)
at
com.tangosol.net.cache.ReadWriteBackingMap$CacheStoreWrapper.loadInternal(ReadWrit
eBackingMap.java:5676)
at
com.tangosol.net.cache.ReadWriteBackingMap$StoreWrapper.load(ReadWriteBackingMap.j
ava:4754)
at com.tangosol.net.cache.ReadWriteBackingMap.get(ReadWriteBackingMap.java:717)
at
com.tangosol.coherence.component.util.daemon.queueProcessor.service.grid.partition
edService.PartitionedCache$Storage.get(PartitionedCache.CDB:10)
at
com.tangosol.coherence.component.util.daemon.queueProcessor.service.grid.partition
edService.PartitionedCache.onGetRequest(PartitionedCache.CDB:23)
at
com.tangosol.coherence.component.util.daemon.queueProcessor.service.grid.partition
edService.PartitionedCache$GetRequest.run(PartitionedCache.CDB:1)
at
com.tangosol.coherence.component.util.DaemonPool$WrapperTask.run(DaemonPool.CDB:1)
at
com.tangosol.coherence.component.util.DaemonPool$WrapperTask.run(DaemonPool.CDB:32
)
at
com.tangosol.coherence.component.util.DaemonPool$Daemon.onNotify(DaemonPool.CDB:66
)
at com.tangosol.coherence.component.util.Daemon.run(Daemon.CDB:42)
at java.lang.Thread.run(Thread.java:745)
]]
```

Solution

This occurs when OAM servers cannot communicate with each other using the coherence port. This is often caused by iptables. The workaround for this issue is as follows:

1. Edit the file `/etc/sysconfig/iptables` on both OAMHOST1 and OAMHOST2 and add the following line:

```
# Generated by iptables-save v1.4.7 on Tue Apr 19 10:02:45 2016
*filter
:INPUT ACCEPT [593:243587]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [614:423013]
-A INPUT -p tcp -m state --state NEW -m tcp --dport 9095 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 9097 -j ACCEPT
COMMIT
```

In the above set of lines, `9095` and `9097` are the coherence ports being used.

2. Save the file and restart the servers.

31.10.5 Troubleshooting Oracle Identity Manager

This section describes some common problems that can arise with Oracle Identity Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 31.10.5.1, "java.io.FileNotFoundException When Running Oracle Identity Manager Configuration"
- Section 31.10.5.2, "ResourceConnectionValidationxception When Creating User in Oracle Identity Manager"
- Section 31.10.5.3, "Oracle Identity Manager Reconciliation Jobs Fail"
- Section 31.10.5.4, "OIM Reconciliation Jobs Fail When Running Against Oracle Unified Directory"
- Section 31.10.5.5, "Cannot Open Reports from OIM Self Service Console"

31.10.5.1 java.io.FileNotFoundException When Running Oracle Identity Manager Configuration

Problem

When you run Oracle Identity Manager configuration, the error `java.io.FileNotFoundException: soaconfigplan.xml (Permission denied)` may appear and Oracle Identity Manager configuration might fail.

Solution

To workaround this issue:

1. Delete the file `/tmp/soaconfigplan.xml`.
2. Start the configuration again (`OH/bin/config.sh`).

31.10.5.2 ResourceConnectionValidationxception When Creating User in Oracle Identity Manager

Problem

If you are creating a user in Oracle Identity Manager (by logging into Oracle Identity Manager System Administration Console, clicking the Administration tab, clicking the **Create User** link, entering the required information in the fields, and clicking **Save**) in an active-active Oracle Identity Manager configuration, and the Oracle Identity Manager server that is handling the request fails, you may see a "ResourceConnectionValidationxception" in the Oracle Identity Manager log file, similar to:

```
[2010-06-14T15:14:48.738-07:00] [oim_server2] [ERROR] [] [XELLERATE.SERVER]
[tid: [ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: xelsysadm] [ecid:
004YGJGmYrtEkJV6u3M6UH00073A0005EI,0:1] [APP: oim#11.1.1.3.0] [dcid:
12eb0f9c6e8796f4:-785b18b3:12938857792:-7ffd-0000000000000037] [URI:
/admin/faces/pages/Admin.jspx] Class/Method:
PooledResourceConnection/heartbeat encounter some problems: Operation timed
out[[
com.oracle.oim.gcp.exceptions.ResourceConnectionValidationxception: Operation
```

```
timed out
        at
oracle.iam.ldapsync.impl.repository.LDAPConnection.heartbeat(LDAPConnection.ja
va:162)
        at
com.oracle.oim.gcp.ucp.PooledResourceConnection.heartbeat(PooledResourceConnec
tion.java:52)
         .
         .
         .
```

Solution

Despite this exception, the user is created correctly.

31.10.5.3 Oracle Identity Manager Reconciliation Jobs Fail

Problem

Oracle Identity Manager reconciliation jobs fail, or one of the following messages is seen in the log files:

- Error-1

  ```
  LDAP Error 53 : [LDAP: error code 53 - Full resync required. Reason: The
  provided cookie is older than the start of historical in the server for the
  replicated domain : dc=example,dc=com]
  ```

- Error-2

  ```
  LDAP: error code 53 - Invalid syntax of the provided cookie
  ```

This error is caused by the data in the Oracle Unified Directory change log cookie expiring because Oracle Unified Directory has not been written to for a certain amount of time.

Solution:

1. Open a browser and go to the following location:

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

2. Log in a as `xelsysadm` using the *`COMMON_IDM_PASSWORD`*.
3. Under **System Management**, click **Scheduler**.
4. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
5. For each job in the search results, click on the job name on the left, then click **Disable** on the right.

   Do this for all jobs. If the job is already disabled do nothing.

6. Run the following commands on LDAPHOST1:

   ```
   cd LDAP_ORACLE_INSTANCE/OUD/bin
   ./ldapsearch -h ldaphost1 -p 1389 -D "cn=oudadmin" -b "" -s base
   "objectclass=*" lastExternalChangelogCookie

   Password for user 'cn=oudadmin': <OudAdminPwd>
   dn: lastExternalChangelogCookie:
   dc=example,dc=com:00000140c682473c263600000862;
   ```

Copy the output string that follows `lastExternalChangelogCookie:`. This value is required in the next step. For example,

```
dc=example,dc=com:00000140c682473c263600000862;
```

The Hex portion must be 28 characters long. If this value has more than one Hex portion then separate the 28char portions with spaces. For example:

```
dc=example,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
```

7. Run each of the following LDAP reconciliation jobs once to reset the last change number.:
   - LDAP Role Delete Reconciliation
   - LDAP User Delete Reconciliation
   - LDAP Role Create and Update Reconciliation
   - LDAP User Create and Update Reconciliation
   - LDAP Role Hierarchy Reconciliation
   - LDAP Role Membership Reconciliation

   To run the jobs:

   a. Login to the OIM System Administration Console as the user `xelsysadm`.
   b. Under **System Configuration**, click **Scheduler**.
   c. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
   d. Click on the job to be run.
   e. Set the parameter **Last Change Number** to the value obtained in step 6.

      For example:

      ```
      dc=example,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
      00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
      ```

   f. Click **Run Now**.
   g. Repeat for each of the jobs in the list at the beginning of this step.
8. For each incremental recon job whose last changelog number has been reset, execute the job and check that the job now completes successfully.
9. After the job runs successfully, re-enable periodic running of the jobs according to your requirements.

If the error appears again after the incremental jobs have been re-enabled and run successfully ("Full resync required. Reason: The provided cookie is older..."), then increase the OUD cookie retention time. Although there is no hard and fast rule as to what this value should be, it should be long enough to avoid the issue, but small enough to avoid unnecessary resource consumption on OUD. One or two weeks should suffice. Run the following command on each OUD instance to increase the retention time to two weeks:

```
cd OUD_ORACLE_INSTANCE/bin

./dsconfig set-replication-server-prop --provider-name "Multimaster
Synchronization" --set replication-purge-delay:2w -D cn=oudadmin --trustAll -p
4444 -h LDAPHOSTn
```

```
Password for user 'cn=oudadmin':  <OudAdminPswd>
Enter choice [f]: f
```

31.10.5.4 OIM Reconciliation Jobs Fail When Running Against Oracle Unified Directory

Problem: Reconciliation jobs fail when running against Oracle Unified Directory (OUD). The following error is seen in the OIM WebLogic Server logs:

```
LDAP: error code 53 - Invalid syntax of the provided cookie
```

Solution: Try out the workaround described in Section 31.10.5.3, "Oracle Identity Manager Reconciliation Jobs Fail". If that does not resolve the issue, try the following solution:

On each OIMHOST, update the *IGD_MSERVER_HOME*`/config/fmwconfig/ovd/oim/adapters.os_xml` file with the following parameter:

```
<param name="eclCookie" value="false"/>
```

Restart the OIM and SOA Managed Servers.

31.10.5.5 Cannot Open Reports from OIM Self Service Console

Problem: The reports cannot be opened from OIM Self Service Console.

Solution: When you enable the Identity Auditor feature in OIM, do the following configuration changes for the OIM-BI Publisher integration to work fine:

1. Log in to the IAMGovernanceDomain Enterprise Management console.
2. Open the system MBean browser and update the MBean `"oracle.iam:Location=wls_oim1,name=Discovery,type=XMLConfig.DiscoveryConfig,XMLConfig=Config,Application=oim,ApplicationVersion=11.1.2.0.0"` with Value as `http://`*`igdadmin.example.com`*`/`.

   Here, *`igdadmin.example.com`* is the Governance Domain admin Load balancer URL.

31.10.6 Troubleshooting Oracle SOA Suite

This section describes some common problems that can arise with Oracle SOA Suite and the actions you can take to resolve the problem. It contains the following topics:

31.10.6.1 Transaction Timeout Error

Problem: The following transaction timeout error appears in the log:

```
Internal Exception: java.sql.SQLException: Unexpected exception while enlisting
 XAConnection java.sql.SQLException: XA error: XAResource.XAER_NOTA start()
failed on resource 'SOADataSource_soaedg_domain': XAER_NOTA : The XID
is not valid
```

Solution: Check your transaction timeout settings, and be sure that the JTA transaction time out is less than the DataSource XA Transaction Timeout, which is less than the `distributed_lock_timeout` (at the database).

With the out of the box configuration, the SOA data sources do not set XA timeout to any value. The `Set XA Transaction Timeout` configuration parameter is unchecked in the WebLogic Server Administration Console. In this case, the data sources use the

domain level JTA timeout which is set to 30. Also, the default distributed_lock_timeout value for the database is 60. As a result, the SOA configuration works correctly for any system where transactions are expected to have lower life expectancy than such values. Adjust these values according to the transaction times your specific operations are expected to take.

31.10.7 General Troubleshooting

This section describes the common issues and their workaround. This section includes the following topic:

- Section 31.10.7.1, "Cannot Start Managed Server from WebLogic Console"
- Section 31.10.7.2, "Proxy Settings are Reset"

31.10.7.1 Cannot Start Managed Server from WebLogic Console

When you start a Managed Server from the WebLogic Console, the following error is shown:

```
. For server WLS_BI1, the Node Manager associated with machine oimhost1 is not
reachable.
. All of the servers selected are currently in a state which is incompatible with
this operation or are not associated with a running Node Manager or you are not
authorized to perform the action requested. No action will be performed.
```

Solution 1

Check if the Node Manager is started on the target host. If not, start it.

Solution 2

Verify that the domain is listed in the file nodemanager.domains, which is located in the directory *SHARED_CONFIG_DIR*/nodemanger/hostname. If not, do the following:

1. Start the WebLogic Scripting Tool (WLST) by running the following command from the location *MW_HOME*/oracle_common/common/bin/:

   ```
   ./wlst.sh
   ```

2. Connect to the domain you wish to add by running the following command:

   ```
   connect('weblogic_user','password','t3://ADMINVHN:AdminPort')
   ```

   In this command:

   weblogic_user is the WebLogic Administration user. For example, weblogic or weblogic_idmw.

   password is the password of the WebLogic Administration user.

   ADMINVHN is the Virtual host name of the Administration Server. For example, IGDADMINVHN or IADADMINVHN.

   adminPort is the port on which the Administration Server is running. For example, 7101.

   Sample Command:

   ```
   connect('weblogic_idm','mypasswd','t3://igdadminvhn.example.com:7001')
   ```

3. Enrol the domain using the following command:

   ```
   nmEnroll(domainDir=absolute_path_to_the_domain,nm_Home=absolute_path_
   to_the_nodemanager_home)
   ```

For example:

```
nmEnroll(domainDir='/u02/private/oracle/config/domains/IAMGovernanceDom
ain/',nmHome='/u01/oracle/config/nodemanger/hostname)')
```

Note: For Managed Servers, the domain home should always be specified as the local managed server directory.

31.10.7.2 Proxy Settings are Reset

Proxy settings are reset after changing via the MSM console. This happens because there is a different configuration file for the admin server and the managed servers.

Solution

1. Locate the `msm-config.xml` file present under the *`$IAD_ASERVER_HOME`*`/config/fmwconfig` directory.
2. Remove or rename the `msm-config.xml` file.

A

Creating a Redundant Middleware Home

The Section 7.5.1.3, "About Using Redundant Binary (Middleware Home) Directories" recommends that you create duplicate Middleware homes to ensure that the middleware home is not a single point of failure. You can not achieve this when using the deployment wizard. You must do it as a separate task after deployment is complete. This appendix describes how to create a duplicate Middleware home.

This appendix contains the following topic:

- Appendix A.1, "Creating a Duplicate Middleware Home"

A.1 Creating a Duplicate Middleware Home

To create a duplicate Middleware home:

1. Make a backup of the Middleware home at the *SW_ROOT* level. For example:

   ```
   tar cvfz mwhomebackup.tar.gz SW_ROOT
   ```

2. Create a new shared file system on shared storage the same way you created the original *SW_ROOT* volume:

   a. Shutdown the entire topology.

   b. Dismount the *SW_ROOT* from your even numbered hosts, where it is mounted.

      For example, currently, *SW_ROOT* is mounted on OAMHOST1, OAMHOST2, OIMHOST1 and OIMHOST2.

      Dismount it from OAMHOST2 and OIMHOST2.

   c. Mount the new SW_ROOT volume onto the even numbered hosts, (OAMHOST2/OIMHOST2) in the same location as *SW_ROOT*.

3. Restore your backup using one of the even numbered hosts. For example, using OAMHOST2:

   ```
   tar xvfz mwhomebackup.tar.gz
   ```

4. Restore your backup using one of the even numbered hosts. For example, using OAMHOST2:

   ```
   tar xvfz mwhomebackup.tar.gz
   ```

Once you have created a duplicate Middleware home, if, for some reason, *SW_ROOT* on OAMHOST1 is corrupted, only OAMHOST1/OIMHOST1 are affected. OAMHOST2 and OIMHOST2 are unaffected. However, now that you have two sets of Middleware homes, you need to use automated patching on each home.

To use automated patching for Oracle Identity Management:

1. Make a backup of the file `topology.xml`.
2. Create a new MW_HOME using the command:

```
topotool.sh add -mwhome -mwhomename Identity:MW_HOME2 -path SW_ROOT/identity
-shared true
```

3. Create a new Oracle Home for each component in the middleware home.

```
topotool.sh add -home -mwhomename Identity:MW_HOME2 -type ORACLE_COMMON -path
SW_ROOT/identity/oracle_common
topotool.sh add -home -mwhomename Identity:MW_HOME2 -type WLS -path SW_
ROOT/identity/wlserver_10.3
topotool.sh add -home -mwhomename Identity:MW_HOME2 -type SOA -path SW_
ROOT/identity/soa
topotool.sh add -home -mwhomename Identity:MW_HOME2 -type IAM -path SW_
ROOT/identity/iam
```

4. Move components to the new Middleware home.

```
topotool.sh modify -instance -name IAMGovernanceDomain:wls_soa2 -mwhomename
Identity:MW_HOME2 -hometype SOA
topotool.sh modify -instance -name IAMGovernanceDomain:wls_oim2 -mwhomename
Identity:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_bi2 -mwhomename
Identity:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_opam2 -mwhomename
Identity:MW_HOME2 -hometype IAM
```

For Oracle Access Management:

1. Create a new *MW_HOME* using the following command:

```
topotool.sh add -mwhome -mwhomename Access:MW_HOME2 -path /SW_ROOT/access
-shared true
```

2. Create a new Oracle Home for each component in the Middleware home.

```
topotool.sh add -home -mwhomename Access:MW_HOME2 -type ORACLE_COMMON -path SW_
ROOT/access/oracle_common
topotool.sh add -home -mwhomename Access:MW_HOME2 -type WLS -path SW_
ROOT/access/wlserver_10.3
topotool.sh add -home -mwhomename Access:MW_HOME2 -type IAM -path SW_
ROOT/access/iam
```

3. Move components to the new Middleware home.

```
topotool.sh modify -instance -name IAMAccessDomain:wls_oam2 -mwhomename
Access:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_ampm2 -mwhomename
Identity:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_msm2 -mwhomename
Identity:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_oaam2 -mwhomename
Identity:MW_HOME2 -hometype IAM
topotool.sh modify -instance -name IAMGovernanceDomain:wls_oaam_admin2
-mwhomename Identity:MW_HOME2 -hometype IAM
```

4. Restart the topology.

B

Sanity Checks

The sanity tests described in this appendix are over and above the normal tests detailed in the guide. They are designed to test the in-depth functionality of Oracle Access Management (OAM) and Oracle Identity Manager (OIM).

This appendix includes the following sections:

- Sanity Checks for Oracle Access Management
- Sanity Checks for Oracle Identity Manager

B.1 Sanity Checks for Oracle Access Management

This section lists the sanity checks for Oracle Access Management (OAM). It includes the following topics:

- Appendix B.1.1, "Verifying LDAP Authentication for OAM Agent Protected Application for Valid User"
- Appendix B.1.2, "Verifying LDAP Authentication Failure for OAM Agent Protected Application for Invalid Password"
- Appendix B.1.3, "Verifying LDAP Authentication Failure for OAM Agent Protected Application for Invalid Username"
- Appendix B.1.4, "Verifying Access of OAM Agent Protected Unavailable Resource"
- Verifying Access of Resource that was Recently Deleted or Replaced from the Policy

B.1.1 Verifying LDAP Authentication for OAM Agent Protected Application for Valid User

To verify the LDAP authentication for OAM agent protected application for valid user, do the following:

1. Access an application protected by an OAM WebGate which is configured to OAM server.
2. Check out the URL that is being redirected to for authentication is from OAM server.
3. Provide a valid username and password from the OID or OUD authentication form and click Login.
4. Check the cookies that are created in the browser.

Expected Result:

- OAM agent protected Application can be accessed on providing valid credentials.
- ObSSOcookie and OAM_ID cookies are created in the browser session.

B.1.2 Verifying LDAP Authentication Failure for OAM Agent Protected Application for Invalid Password

To verify the LDAP authentication failure for OAM agent protected application for invalid password, do the following:

1. Access an application protected by an OAM WebGate which is configured to OAM server.
2. Check out the URL that is being redirected to for authentication is from OAM server.
3. Provide a valid username and an invalid password in the authentication form.

Expected Result:

- User authentication fails.
- Appropriate error message is displayed.
- Resource cannot be accessed by the user.

B.1.3 Verifying LDAP Authentication Failure for OAM Agent Protected Application for Invalid Username

To verify the LDAP authentication failure for OAM agent protected application for invalid username, do the following:

1. Access an application protected by an OAM WebGate which is configured to OAM server.
2. Check out the URL that is being redirected to for authentication is from OAM server.
3. Provide an invalid username and any password in the authentication form.

Expected Result:

- User authentication fails.
- Appropriate error message is displayed.
- Resource cannot be accessed by the user.

B.1.4 Verifying Access of OAM Agent Protected Unavailable Resource

If you access an OAM agent protected unavailable resource, an appropriate error message is displayed though the credentials provided are valid. To verify this, do the following:

1. Access a resource url protected by an OAM WebGate which is configured to OAM server when that resources is not available.
2. Check out the URL that is being redirected to for authentication is from OAM server.
3. Provide a valid username and password in the authentication form.
4. Check the cookies that are created in the browser.

Expected Result:

OAM WebGate protected application cannot be accessed and a proper error message should be displayed.

B.1.5 Verifying Access of Resource that was Recently Deleted or Replaced from the Policy

If you access a resource which was recently deleted or replaced from the policy, the authentication is not required and the access is granted. To verify this, do the following:

1. Remove a resource and replace it with new one in the `policy.xml` or UI.
2. Access the application or resource that you deleted or replaced in the previous step. This application must be protected by an OAM WebGate which is configured to OAM server.
3. Check if the user is not asked for authentication without having to restart the OAM 11*g* Server or WebLogic Server.
4. Check if user is able to access the resource.

Expected Result:

Resource or Application can be accessed without having to authenticate user and without having to restart the OAM 11*g* Server or WebLogic Server.

B.2 Sanity Checks for Oracle Identity Manager

This section lists the sanity checks for Oracle Identity Manager. It includes the following topics:

- Creating Organization
- Creating User
- Creating Role
- Self-Registering a User
- Adding User Defined Field (UDF) in User
- Creating Disconnected Application and Provision
- Importing and Configuring DB User Management
- Creating Access Policy and Provision
- Creating End User Request for Accounts, Entitlements, and Roles
- Resetting Account Password
- Creating Certification and Approving
- Creating Identity Audit Scan Definitions and Viewing its Results
- Testing Identity Audit

B.2.1 Creating Organization

To create an organization, do the following:

1. Log in to the Identity console as `xelsysadm` using the following URL:

   `https://`prov.example.com`/identity`
2. Click **Manage**, and then click **Organization**.

3. Click **Create Org**, and specify the org name as Pepsi.

B.2.2 Creating User

To create a user, do the following:

1. Log in to the Identity console as `xelsysadm` using the following URL:

   `https://prov.example.com/identity`

2. Click **Manage**, and then click **User**.
3. Click **Create User**, and specify the user name as Rahul Dravid.
4. Select Org as Pepsi.
5. Log in as Rahul Dravid.
6. Set the challenge questions and answers.
7. Verify successful login to the Identity console.

B.2.3 Creating Role

To create a role, do the following:

1. Log in to the Identity console as `xelsysadm` using the following URL:

   `https://prov.example.com/identity`

2. Click **Manage**, and then click **Role**.
3. Click **Create** and provide the mandatory attributes (Name, Display Name) to create a Role named `Coach`, and click **Next**.
4. Click Next.
5. On the **Organizations** page, click **Add Organizations**. Provide the organization name as **Pepsi** and click **Search**.
6. Select the organization **Pepsi** and click **Add Selected**. Click **Select**.
7. Click **Next**, and then click **Finish**.

B.2.4 Self-Registering a User

To self-register a user, do the following:

1. Access the Identity console URL. For example:

   `https://prov.example.com/identity`

   Do not log in.

2. Click the **Self-Registration** link on the login page.
3. Enter the user login, lastname, email, challenge question, password, and Click **Register**.
4. Log in to the Identity console as `xelsysadm`.
5. Approve the self-registration request.
6. Verify email notification for self-reg from the inbox.
7. Log out and relog-in as self-reg user.

B.2.5 Adding User Defined Field (UDF) in User

To add User Defined Field (UDF) in user, do the following:

1. Log in to the System Administration console as `xelsysadmin` using the following URL:

   `http://IGDADMIN.example.com/sysadmin`

2. Create & Activate Sandbox.
3. Open **User** form under **System Entities**.
4. Click **Create** icon.
5. Select **Text**.
6. Populate **Display Label** and **Name**, select **Searchable**, and save form.
7. Publish **Sandbox**.
8. Log in to the Identity console as `xelsysadm` using the following URL:

   `http://prov.example.com/identity`

9. Create and Activate Sandbox.
10. Open Users page, and click **Create**.
11. Populate mandatory attributes - Organization, User Type, Last Name.
12. Click **Customize** and, go to the **Structure** tab.
13. Select **Basic information** as panelFormLayout.
14. Click **Add**.
15. Select **Data Component - Catalog**, and then click **UserVO**.
16. Select the udf and select **ADF Input Text w/ Label**.
17. Close form.
18. Search any user and open user details page.
19. Click **Customize** link and go to the **Structure** tab.
20. Select **Basic information** as the panelFormLayout.
21. Click **Add**.
22. Select **Data Component**, and then select **Manage Users**, and **UserVO1**.
23. Add the udf by selecting **ADF Output Formatted w/ Label**.
24. Close the structure form by clicking **Close** on the top right corner of the Identity console window.
25. Open any user, and click **Modify**.
26. Click **Customize** link and go to the **Structure** tab.
27. Select **Basic information** as the panelFormLayout.
28. Click **Add**.
29. Select **Data Component - Catalog**, and then **UserVO1**.
30. Click **Add** next to the udf that was created in step 6 and select **ADF Input Text w/ Label** option.
31. Select **First Name** and click the **Show Properties** icon.

32. Copy the **Value Change Listener** of first name attribute. For example:

    `#{pageFlowScope.cartDetailStateBean.attributeValueChangedListener`

    Dismiss the properties page.

33. Select the udf that you just added, and click **Edit Properties**.

34. Select **Auto-Submit**, and add the **Value Change Listener** value that you copied in 32.

35. Click **OK** to apply the updates and close the form.

36. Publish the Sandbox.

37. Log out and log in again.

38. Open the user details page.

39. Create a user populating udf attribute and verify if it is displayed properly in user details page.

40. Modify the UDF attribute and verify if it is displayed properly.

B.2.6 Creating Disconnected Application and Provision

To create disconnected app and provision, do the following:

1. Create a lookup by completing the following steps:
    a. Log in to the System Administration console as `xelsysadm` using the following URL:

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

    b. Go to **System Configuration** tab and click **Lookups**.

    c. Click the **Create Lookup Type** icon. Create lookup type pop is displayed.

    d. Enter the meaning as `Lookup.Disc`, and enter the code as `Lookup.Disc`.

    e. Click on **Create lookup code** button.

    f. Enter the value `HDD` for Meaning, and `HDD` for Code, and check **Enabled**.

    g. Click **Save**.

    h. Click **Select and Search**.

    i. Enter the value `Lookup.Disc` for Meaning, `Lookup.Disc` for code, and click **Search**.

    j. The values **HDD** and **CD** are displayed. Click **OK**.

2. Create disconnected application instances by completing the following steps:
    a. Log in to the System Administration console as `xelsysadm` using the following URL:

       `http://igadmin.example.com/sysadmin`

    b. Click the **Sandboxes** link, and then click **Create Sandbox**.

    c. Enter the name **Disc**, and click **Save** and **Close**. Click **OK** to confirm. Sandbox is activated.

    d. Go to **Provisioning configuration**, and click **Application Instances**.

    e. Click **Create**. The Create App Instance page is displayed by enabling the Attribute tab.

f. Enter the name as **Disc**, Description as **Disc**, and check the **Enabled Disconnected** check box. Click **Save**. Click **OK** to confirm. Feedback message is displayed to confirm that Application Instance Disc is created successfully.

g. On the same page, go to the **Attribute** tab. Form field is added with the name **Disc**. Click **Edit** next to Form field.

h. Enable the **Field** tab and open Manage Disc page. Click **Child objects** which is next to the Field tab.

i. Click **Add**, and enter the name as **chdisc**, description as **chdisc**, and Click **OK**.

j. Click **chdisc**. This opens another page by enabling the **Fields** tab.

k. Click **Create a Custom Field** and select **Lookup** as the Field type, and click **OK**.

l. Enter the Display name `Disc`. **Name** field will populate a value automatically, You do not have to enter another name for Name. Enter the description as `Disc` and check **Enabled Searchable**. Click **Lookup Type**, and then click **Search** or look up icon (Magnifier icon). Enter the meaning as `Lookup.Disc`.

m. Click **Search**. Values **HDD** and **CD** must be displayed. Click **OK**. Lookup must be selected. Default Value Label, One Drop down gets added. Click on that, and you will see the values: HDD and CD.

If you enabled **Entitlement**, make sure that **Searchable** and **Searchable Picklist** are also selected. Keep the remaining ones with the default values.

n. Click **Save** and then click **Close**.

o. Click **Back to Parent Object**, and then click **Regenerate view**.

p. Enable **Parent Form + Child Tables (Master/Detail)**, keep the default setting. Click **OK**.

q. Go to the **Application Instance** tab. Search for an Application Instance **Disc**.

r. Click **Refresh**, and click **Apply** on Disc form.

s. Go to the **System Configuration** tab, and click **Scheduler**.

t. Enter the value **Ent*** in the **Search Scheduled Jobs** field, click **Search** or **Go** button.

u. The results are displayed. Click on Entitlement List job name.

v. Click **Run now**. A confirmation message is displayed saying the Job is running.

w. Click **Refresh.** Verify that the execution status is successful. Close the window.

x. Go to the Application instance's Entitlement tab. Two entitlements are displayed - HDD, CD.

y. Search organization name, by entering the value Top, and click **Search**.

z. Top organization should be displayed. Select that row / organization, and click **Add Selected**. Selected organization gets added successfully.

aa. Check **Apply to Entitlement**, and click **Select**. Selected Organization gets added successfully.

ab. Click **Assign**.

ac. Search for the organization name **Pepsi**, and click **Search**.

ad. Pepsi organization is displayed. Select that row / organization, and click **Add Selected**.

ae. Selected organization gets added successfully. Check **Apply to Entitlement** and click **Select**. Selected organization gets added successfully.

af. Go to the Application Instance's Attribute tab. Click **Apply**. A message is displayed stating that the Application instances disc is modified successfully.

ag. Click Sandboxes.

ah. Select the same sandbox **Disc**. Click **Export sandbox** button. Export sandbox generate .zip file `sandbox_disc.zip`. Click **OK** button. Zip file is saved and generated.

ai. After export is successfully completed, click **Publish sandbox** button. Click **Yes** to confirm.

aj. After you publish, the sandbox is listed under Publish Sandboxes link.

3. Provision the disconnected application instances and entitlements to user by completing the following steps:

a. Log in to the Identity console as `xelsysadm` using the following URL:

`https://prov.example.com/identity`

b. Click **Manage** and then click **Users**.

c. Search for the user name `Rahul Dravid`, and click **Search**.

d. The user Rahul Dravid is displayed. Click on that user link. User details are displayed.

e. Go to **Accounts** tab, and then to the **Request Account** tab. Account access request page is displayed. Select **Enabled Add access**., and go to the **Catalog** tab. All available Application Instances are displayed.

f. Click **Add to cart** of the **Disc** Disconnected application instances, and click **Next**. The cart detail page is displayed

g. Click the Pen Icon on Request detail pane.

h. Enter the account logging name as `Rahul Dravid_123`, and the password as `Welcome1`. Click **Update**.

i. Click **Submit**. Request will be generated with a message `Request for access completed successfully`.

j. Go to the **Self Service** tab. Click **Provisioning task**, and the go to the **Manual Fulfillment** tab. Manual fulfillment page is displayed.

k. Click on that request. Request details are displayed. Verify the data. Click **Complete**, and then click **Refresh**.

l. Go to the **Manage** tab, and then to the **User** tab. Open the same user Rahul Dravid.

m. Go to the **Account** tab. Click **Refresh**. Verify that the account status is `Provisioned`.

n. Select the same account name Rahul Dravid_123, and click Request Entitlement button. Entitlement Access request page is displayed. Enable **Add Access** and go to the **Catalog** tab.

o. Click **Add to cart** for entitlement `HDD`. Click **Next**.

p. Click **Submit**. Request will be generated with a message "Request for access completed successfully".

q. Go to the **Self service** tab. Click on **Provisioning task**, and go to **Manual Fulfillment** tab. Manual fulfillment page is displayed

r. Click on that request. Request details are displayed. Verify the data. Click **Complete**, and then click **Refresh**.

s. Go to the **Manage** tab, and then to the **User** tab. Open the same user Rahul Dravid.

t. Go to the **Entitlement** tab. Click **Refresh** button. Verify that the Entitlement status is `Provisioned`.

B.2.7 Importing and Configuring DB User Management

To import and configure Database user management, do the following:

1. Download the latest Database User Management Connector from the Oracle Identity Manager Connector Downloads page on Oracle Technology Network (OTN):

   `http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html`

2. Log in to the System Administration console as `xelsysadmin` user using the following URL:

   `http://`*`igdadmin.example.com`*`/sysadmin`

3. Go to the **System Configuration** tab and click **Import**.

4. Select the file `DBUserManagement-Oracle-ConnectorConfig.xml`'. Sample location: `D:\DBUM11.1.1.6\DBUM-11.1.1.6.0\DBUM-11.1.1.6.0\xml`

5. Click **Add**.

6. Click **Next**. You can either provide the ITResource details now or later. To provide the same later, click **Skip**.

7. Click **View Selections**, and click **Import**. Once the import is successfully completed, click **OK**.

8. Copy the third party jars of target systems to the *`OIM_HOME`*`/server/ConnectorDefaultDirectory/targetsystems-lib/DBUM-11.1.1.6.0` directory.

   Note: :If the target is Oracle database, no driver jar is needed.

9. To configure a trusted source reconciliation, create and configure a new IT resource. For example, Oracle DB Trusted of type Oracle DBUM.

10. In the Configuration Lookup, update the trusted configuration lookup name as `Lookup.DBUM.Oracle.Configuration.Trusted`. This configures the ITResource for the target system.

11. Either you can create the ITResource and provide the following details or Open the existing ITResource 'Oracle DB' as specified below:

    ITResource Details:

    `Configuration Lookup = Lookup.DBUM.Oracle.Configuration`

`Connector Server Name =`

`Connection Properties =` Specify the connection properties for the target system database.

`Database Name =` This field identifies database type (such as Oracle and MSSQL) and its used for loading respective scripts. Sample value: Oracle

`JDBC Driver = oracle.jdbc.driver.OracleDriver`

`JDBC URL =` For Oracle: `jdbc:oracle:thin:@host:port:sid`

`Login Password =` Enter the password for the user name of the target system account to be used for connector operations.

`Login User = sys as sysdba`

B.2.8 Creating Access Policy and Provision

To create an access policy and provision, do the following:

1. Create a Role named `DBUMRole`.
2. Create an user named `Jean Wilson`.
3. Assign the role `DBUMRole` to `Jean Wilson`.
4. Log in to system administration console.
5. Open Access Policies page under **Policies**.
6. Click **Create Access policy** on Manage page.
7. Populate the following:

   `Access Policy Name :` DBUM Policy

   `Access Policy Description :` Policy to provision DBUM App to users

   `Retrofit Access Policy : true`
8. Click **Continue**.
9. Select **Resources** page, and select the DBUM resource and continue.
10. On the Provide Resource Data page, select the IT resource attribute, and click **Set Additional data**.
11. Select two or more child data and click **Continue**.
12. Select **Revoke if no longer applies** and click **Continue**.
13. In "Step 3: Select Resources - Specify the resources to be denied by this access policy" - DONOT select any resource. Click **Continue**.
14. Click **Create Access policy**.
15. Create another user named `Patrick Morgan` and assign the user role `DBUMRole`.
16. Log in to system administration console and run scheduler job **Evaluate User Policies**.
17. Open the user details page of Jean Wilson and click **Accounts** tab. DBUM Account should be in Provisioned state.
18. Go to the **Entitlements** tab and verify all child data added in step 11 are displayed.
19. Repeat the previous two steps for user Patrick Morgan.

B.2.9 Creating End User Request for Accounts, Entitlements, and Roles

To create an end user request for roles, do the following:

1. Create a user `Arthur Hill`.
2. Log in as `Arthur Hill` and open **My Access** page, and then **Roles**.
3. Click **Request roles** and in catalog, add **DBUMRole** to cart.
4. Submit request.
5. Log in as administrator and open inbox.
6. Open the request and approve.
7. As `Arthur Hill`,verify that the role is assigned successfully.

To create an end user request for accounts, do the following:

1. Create a user `Bruce Parker`.
2. Log in as `Bruce Parker` and open **My Access** page, and then **Roles**.
3. Click **Request Accounts**.
4. From the Catalog, select the **DBUM App** and add to cart.
5. On the submission page, populate the form fields and submit request.
6. Log in as administrator and open Inbox.
7. Open the request, verify the details, and approve request.
8. As `Bruce Parker`, verify that the Account is provisioned successfully.

To create an end user request for entitlements, do the following:

1. Log in as `Jean Wilson`.
2. Open the **My Access** page and go to the **Accounts** tab.
3. Select the **DBUM app**, and click **Request Entitlements**.
4. Add any entitlement to cart and submit request.
5. Log in as administrator and open Inbox.
6. Open the request and approve.
7. As Jean Wilson, verify that the entitlement is provisioned successfully.

B.2.10 Resetting Account Password

To reset the account password, do the following:

1. Log in to the Identity console as `Jean Wilson`.
2. Click **My Access** and go to the **Accounts** tab.
3. Select **DBUM App** and click **Reset Password**.
4. Provide a new password and submit.
5. Log out and re-login as `xelsysadm`.
6. Click **Manage** and then click **Users**.
7. Search for Jean Wilson and open the user details page.
8. Go to the **Accounts** tab and select **DBUM App**.

9. Click **Resource profile history** and check if the Password Updated task is triggered and is in Completed status.

B.2.11 Creating Certification and Approving

In order to create certification and approve, you must complete the following prerequisites:

1. Log in to Identity console by `xelsysadm`.
2. Launch the System Administration console.
3. Go to the **System Configuration** tab and click **Configuration Properties**.
4. Look for the following system properties:

   ```
   Property name = Identity Auditor Feature Set Availability

   Keyword = OIG.IsIdentityAuditorEnabled

   Value = TRUE
   ```

5. Save the setting.
6. Restart the OIM server to see the Compliance tab in Identity console.

To create a certification and approve, do the following:

1. Log in to the Identity console as `xelsysadm`.
2. Go to **compliance**, **Certification**, and then **Definitions**.
3. Create a user type certification with the following information:
   - General details page: Enter the name = `UserCertification`, Type = `user`; Enter Description and click **Next**.
   - Base Selection page: Selected Organization and Add organization (Pepsi). Added organization is displayed. Select **Any Level** as Risk Level, and click **Next**.
   - Content selection page: Keep the default values, and click **Next**.
   - Configuration page: Keep the default and click **Next**.
   - Select the reviewer by searching for a user, for example, MSDhoni, and click **Next**.
   - Disable Incremental, and click **Next**.
   - Summary page: Click **Create**, and click **Yes** to confirm. Certification is created successfully.
4. Log in to the System Administration console as xelsysadm.
5. Click **Scheduler**.
6. Search for a certification `cert_UserCertification`. Verify that the job is run successfully.
7. Log in to the Identity console as xelsysadm, and log out from the xelsysadm.
8. Log in to the Identity console as reviewer (MSDhoni).
9. Go to **Self service**, and click **Certification**.
10. Open the same certification **UserCertification [MSDhoni]**.
11. Certification details are displayed. You will see the user "Rahul Dravid".

12. Click on Rahul Dravid user.
13. Verify, Role - Coach, Account - Disc, Entitlement - HDD.
14. Select all rows, and take the Certify action. Sign-off pop up should be displayed
15. Enter the password (username = MSDhoni ; Password = Welcome1). Click **OK**. Certification is completed successfully. It should now reflect in your Inbox. It will be displayed under the Completed section.
16. Log in to the Identity console as MSDhoni / Xelsysadm.
17. Go to **Complaince**, **Certification**, and then **Dashboard**. Dashboard details are displayed.
18. Select **Completed** from the Show Label. This displays all of the completed certifications.

B.2.12 Creating Identity Audit Scan Definitions and Viewing its Results

In order to create identity audit scan definitions, complete the following prerequisites:

1. Log in to the Identity console as `xelsysadm`.
2. Launch the Sysadmin console.
3. Go to the **System Configuration** tab, and click **Configuration Properties**.
4. Look for the following system properties:

   ```
   Property name = Identity Auditor Feature Set Availability
   Keyword = OIG.IsIdentityAuditorEnabled
   Value = TRUE
   ```

5. Save the setting.
6. Restart the OIM server to See the Compliance tab in the Identity console.

Create a rule by doing the following:

1. Log in to the Identity console as `xelsysadm`.
2. Click **Compliance**, and then click **Identity Audit**.
3. Select **Rules**, and click **Create**.
4. Create an identity rule `Identity Rule 1` by the following condition builder:

   ```
   user.Display Name; Equals ; Rahul Dravid
   ```

5. Click **Create**. The rule is created.

Create a policy by doing the following:

1. Log in to the Identity console as `xelsysadm`.
2. Click **Compliance** and then click **Identity Audit**.
3. Click **Policies**, and click **Create**.
4. Create a policy `Identity Policy 1` by adding the rule `Identity Rule 1`.
5. Click **Create**.

Create scan definition by doing the following:

1. Log in to the Identity console as `xelsysadm` using the following URL:

   `https://`*`prov.example.com`*`/identity`

2. Click **Compliance** and then click **Identity Audit**.
3. Click **Scan definitions**, and then click **Create**.
4. Create a scan definition `Identity Scan 1` by adding the policy `Identity Policy 1`.
5. On the Base selection page, select all users.
6. On the Configuration page, keep the default values.
7. On the Summary page, click **Finish**. Scan definition is added successfully.
8. Run the scan definition by selecting **Identity Scan 1**, and clicking **Run now**. Verify that the scan definition is run successfully.
9. Preview the scan definition result by doing the following:
   a. After you run the scan definition, select the scan definition row or record **Identity Scan 1**.
   b. Click **View Scan**. The scan definition results are displayed.

B.2.13 Testing Identity Audit

Complete the following steps to enable audit feature in Oracle Identity Manager:

1. Log in to the System Administration console.
2. Click **System Properties** under **System Configuration**.
3. Search for the property `OIG.IsIdentityAuditorEnabled` and update the property value to `TRUE`.
4. Restart the Oracle Identity Manager Managed Server for the change to take effect.
5. Log in to the Identity console as `xelsysadm` using the following URL:

   `https://prov.example.com/identity`
6. Click **Compliance** and then click **Reports**.

   Verify that the Reports page is opened successfully.

C

Configuring External Access to an Internal Exalogic IAM Deployment

This chapter describes how to configure an Exalogic Identity and Access Management deployment so that it can communicate with applications outside of the Exalogic rack.

If you have configured your Exalogic Identity and Access Management deployment to use the internal network of the Exalogic machine, then you have configured a fully functioning deployment for all applications that are deployed within the Exalogic rack. This configuration, however, does not enable you to protect applications outside of the Exalogic rack, because the security agents cannot talk to the Oracle Access Management Access Manager servers, which are only available on the internal Exalogic network.

In order to achieve a deployment where you have an external agent such as Oracle WebGate protecting a third party application such as SOA or Web Center, you must enable the external agent to communicate with the OAM servers using the public access network. To do this you need to perform the following additional steps.

First, ensure that your Exalogic Compute Nodes or vServers have access to the external Client Access Network using EoIB.

By default, your configuration is configured so that SSO agents communicate with the Access Manager servers, identified as host names iamhost1 and iamhost2, using the internal network.

In summary the steps you must perform are:

1. Create Access Manager server instances registered using the client access network names for those servers.
2. Create an SSO agent inside Access Manager which uses the external Access Manager servers.
3. Configure the external WebGate to use the external SSO agent.

The example in this appendix shows how to protect a simple HTML test page on an external OHS using web gate. It includes the following sections:

C.1 Creating New OAM Server Instances Listening on the External Network

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad, click **Server Instances**.
3. When the search window is displayed, click **Search**.

   You will see your existing server instances displayed: wls_oam1 and wls_oam2.
4. Create two new server instances by clicking the **Create** button and entering the appropriate information. This example shows the values for wls_oam1_ext:
   - **Server Name**: `wls_oam1_ext`
   - **Host**: `iamhost1ext.mycompany.com` (Use the name associated with the client access network.)
   - **Port**: `14000` (*`OIM_PORT`*)
   - **Proxy Server Id**: `AccessServerConfigProxy`
   - **Proxy Port**: `5575` (*`OAM_PROXY_PORT`*)
   - **Mode**: `Simple`

   Leave all other values as they are and click **Apply**.
5. Repeat for Server Name wls_oam2-ext.

You now have four Access Manager server instances, two listening on the internal network and two listening on the external network.

C.2 Creating a New SSO Agent

You can use either `rreg` or the OAM console to create a new SSO Agent. For the purposes of this example we will create a new SSO Agent using the console and using the existing Application Domain IAMSuiteAgent, but for your applications how you create the agent will be dependent on the application you are protecting. Refer to your product documentation for details.

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad, click **SSO Agents**.
3. Click **Create 11g Webgate**.
4. Create with the same values as the existing agent Webgate_IDM_11g, except for these three values:
   - **Name for Example**: `Webgate_External`
   - Deselect **Auto Create Policies**.
   - **Host Identifier** `IAMSuiteAgent`
5. Click **Apply a new web gate agent called Webgate_External**.
6. Edit the newly created agent by clicking **SSO Agents** from the Launch Pad.
7. Click **Search**.
8. Click on the newly created agent **Webgate_External**.

9. Remove all servers from the Primary Server list other than wls_oam1-ext and wls_oam2-ext
10. Click **Apply**.

C.3 Creating a Test Resource in OAM

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 31.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad click **Application Domains**.
3. When the Search Application Domains Window is displayed, click **Search**.
4. Click on the **Application Domain IAM Suite Agent**.
5. Click **Resources** tab.
6. Click **New Resource** and enter the following information:
   - **Type**: `Http`
   - **Description**: `Test Resource`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/sso.html`
   - **Protection Level**: `Protected`
   - **Authentication Policy**: `Protected Higher Level Policy`
   - **Authorization Policy**: `Protected Resource Policy`
7. Click **Apply**.

C.4 Configuring the External Oracle HTTP Server

Install and configure Oracle HTTP server on your external server.

Create a test HTML page called `sso.html` and place it in the OHS `htdocs` folder.

Install WebGate on your external server.

Deploy WebGate to Oracle HTTP, as follows:

1. Execute the command `deployWebGateInstance.sh` which is located in:

   WEBGATE_ORACLE_HOME`/webgate/ohs/tools/deployWebGate`

   The command takes the following arguments:

   - Oracle HTTP instance configuration directory
   - WebGate home directory

   For example:

   ```
   ./deployWebGateInstance.sh -w WEB_ORACLE_INSTANCE/config/OHS/component_name -oh
   WEBGATE_ORACLE_HOME
   ```

2. Set the library path.

   For example, set the library path to include the *WEB_ORACLE_HOME*`/lib` directory as follows

   ```
   export LD_LIBRARY_PATH=LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
   ```

3. Change directory. For example:

   ```
   cd WEBGATE_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools
   ```

4. Run the following command to copy the file `apache_webgate.template` from the WebGate home directory to the WebGate instance location (renamed to `webgate.conf`) and update the `httpd.conf` file to add one line to include the name of `webgate.conf`.

   ```
   ./EditHttpConf -w WEB_ORACLE_INSTANCE/config/OHS/component_name -oh WEBGATE_
   ORACLE_HOME
   ```

5. Copy the files `ObAccessClient.xml`, `cwallet.sso`, and `password.xml`, which were generated when you created the external agent from the directory

   IAD_ASERVER_HOME`/output/Webgate_External`

   on IDMHOST1, to the directory:

   WEB_ORACLE_INSTANCE`/config/OHS/component_name/webgate/config`

6. Copy The files `aaa_key.pem` and `aaa_cert.pem`, which were generated when you created the agent from the directory

   IAD_ASERVER_HOME`/output/Webgate_External`

   on IDMHOST1 to the WebGate instance directory:

   WEB_ORACLE_INSTANCE`/config/OHS/component_name/webgate/config/simple`

7. Restart the Oracle HTTP Server

C.5 Validating the Installation

Test the installation by trying to access the protected resource:

`http://external_ohs/sso.html`

You are redirected to the OAM credential collector. Enter a valid user name and password. The test page is displayed.