Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E12035-02

June 2009

ORACLE®

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management, 11*g* Release 1 (11.1.1)

E12035-02

Primary Author: Bert Rich

Contributing Authors: Bharath K. Reddy, Susan Kornberg, Pradeep Bhat, Xiao Lin, Stephen Lee, Eileen He, Janga Aliminati, Ajay Keni

Contributors: Ellen Desmond, Don Biasotti, Vinaye Misra, Gail Flanegin, Larry Carpenter, Fermin Castro Alonso, Viv Schupmann, Shari Yamaguchi

Contents

3 Creating the WebLogic Server Domain for Identity Management

4 Installing and Configuring OID and OVD

5 Installing and Configuring Oracle DIP and ODSM

6 Installing and Configuring the Web Tier

7 Installing and Configuring Oracle Access Manager

8 Configuring Single Sign-On for Administration Consoles

9 Enabling Administration Server High Availability

10 Managing Enterprise Deployments

Index

Preface

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

Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Fusion Middleware enterprise deployments.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

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

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Security Guide*
- *Oracle Access Manager Introduction*
- *Oracle Access Manager Installation Guide*
- *Oracle Access Manager Access Administration Guide*
- *Oracle Access Manager Identity and Common Administration Guide*
- *Oracle Access Manager Integration Guide*

Conventions

The following text conventions are used in this document:

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

1 Enterprise Deployment Overview

Oracle Identity Management presents a comprehensive suite of products for all aspects of identity management. In the context of Oracle Fusion Middleware, the Oracle Identity Management Infrastructure described in this book primarily includes Oracle Access Manager and Oracle Internet Directory (and/or Oracle Virtual Directory). The directory services provide core LDAP support for both authentication and authorization support in conjunction with Oracle Platform Security Services. Oracle Access Management is the recommended solution for single sign-on across Oracle Fusion Middleware components.

This guide describes a reference enterprise topology for the Oracle Identity Management Infrastructure components of Oracle Fusion Middleware. It also provides detailed instructions and recommendations to create the topology by following the enterprise deployment guidelines.

This chapter includes the following topics:

1.1 What is an Enterprise Deployment?

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

An Oracle Fusion Middleware enterprise deployment:

- Considers various business service level agreements (SLA) to make high-availability best practices as widely applicable as possible
- Leverages database grid servers and storage grid with low-cost storage to provide highly resilient, lower cost infrastructure
- Uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs

- Enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster
- Evolves with each Oracle version and is completely independent of hardware and operating system

For more information on high availability practices, visit:

http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm

1.2 Terminology

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

Table 1–1 Oracle Fusion Middleware Architecture Terminology

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

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

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

1.3 Benefits of Oracle Recommendations

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

1.3.1 Built-in Security

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

- All external communication received on port 80 is redirected to port 443.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the data tier DMZ is allowed.
- Components are separated between DMZs on the web tier, application tier, and the directory tier.
- Direct communication between two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory is isolated in the directory tier DMZ.
- Identity Management components are in the DMZ.
- All communication between components across DMZs is restricted by port and protocol, according to firewall rules.

1.3.2 High Availability

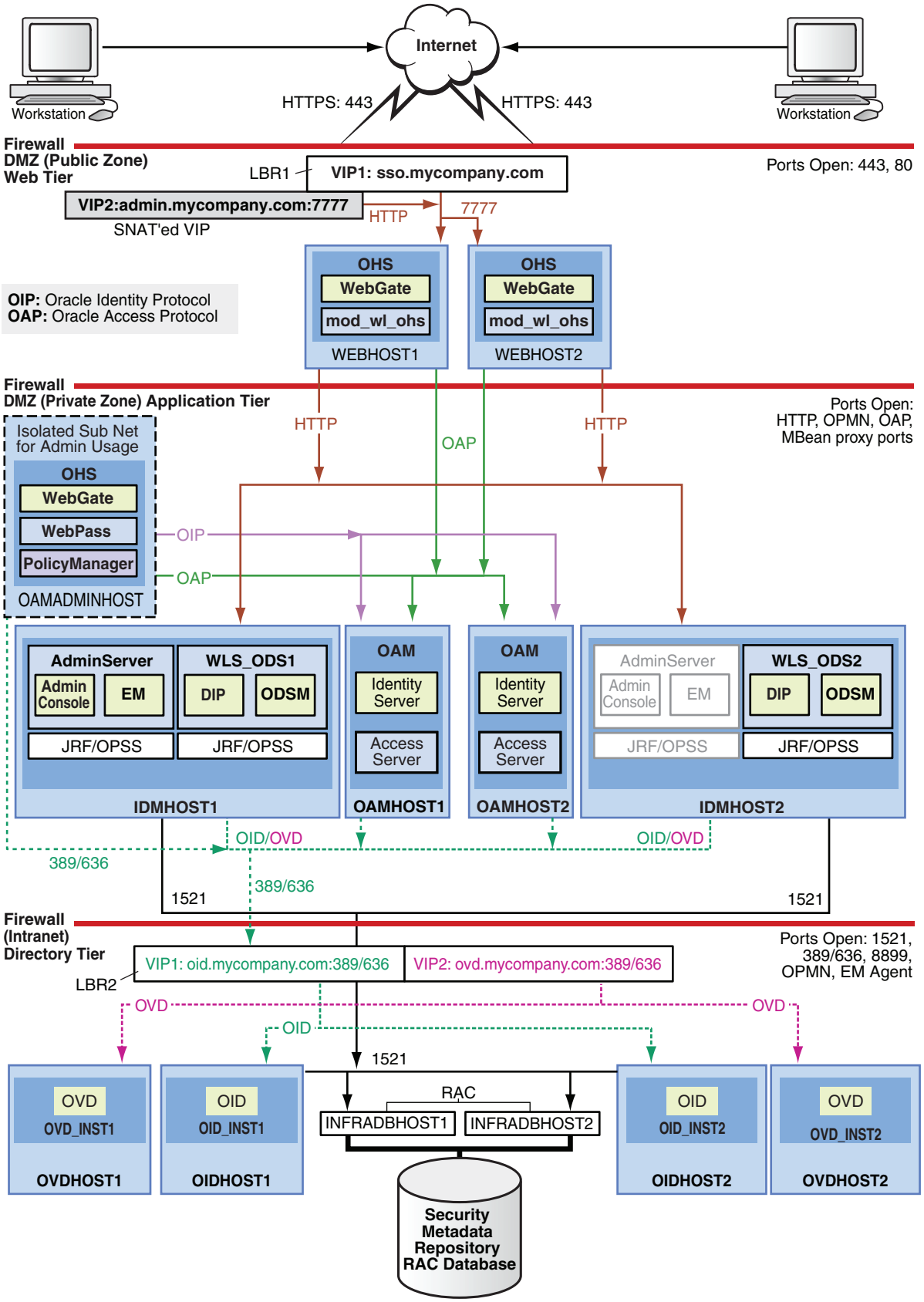
The Enterprise Deployment architectures are highly available, because each component or functional group of software components is replicated on a different computer, and configured for component-level high availability.

1.4 The Enterprise Deployment Reference Topology

The instructions and diagrams in this guide describe a reference topology, to which variations may be applied.

This guide provides configuration instructions for an Oracle Identity Management Infrastructure enterprise deployment using the directory services product and Oracle Access Manager, as shown in Figure 1–1.

Figure 1–1 MyCompany Topology with Oracle Access Manager


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
LBR1
VIP1: sso.mycompany.com
Ports Open: 443, 80
VIP2:admin.mycompany.com:7777
SNAT'ed VIP
HTTP
7777
OHS
WebGate
mod_wl_ohs
WEBHOST1
OHS
WebGate
mod_wl_ohs
WEBHOST2
OIP: Oracle Identity Protocol
OAP: Oracle Access Protocol
Firewall
DMZ (Private Zone) Application Tier
Ports Open:
HTTP, OPMN, OAP,
MBean proxy ports
HTTP
OAP
HTTP
Isolated Sub Net
for Admin Usage
OHS
WebGate
WebPass
PolicyManager
OAMADMINHOST
OIP
OAP
AdminServer
Admin Console
EM
WLS_ODS1
DIP
ODSM
JRF/OPSS
JRF/OPSS
IDMHOST1
OAM
Identity Server
Access Server
OAMHOST1
OAM
Identity Server
Access Server
OAMHOST2
AdminServer
Admin Console
EM
WLS_ODS2
DIP
ODSM
JRF/OPSS
JRF/OPSS
IDMHOST2
OID/OVD
OID/OVD
389/636
1521
389/636
1521
Firewall
(Intranet)
Directory Tier
Ports Open: 1521,
389/636, 8899,
OPMN, EM Agent
LBR2
VIP1: oid.mycompany.com:389/636
VIP2: ovd.mycompany.com:389/636
OVD
OVD
OID
1521
RAC
OVD
OVD_INST1
OVDHOST1
OID
OID_INST1
OIDHOST1
INFRADBHOST1
INFRADBHOST2
OID
OID_INST2
OIDHOST2
OVD
OVD_INST2
OVDHOST2
Security
Metadata
Repository
RAC Database

The computers in the myIDMCompany topology are grouped into the directory tier, application tier, and web tier. These tiers are described in the following sections.

1.4.1 Understanding the Directory Tier

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

The directory tier is closely tied with the data tier, therefore access to the data tier is important:

- Oracle Internet Directory relies on RDBMS as its backend.
- Oracle Virtual Directory provides virtualization support for other LDAP services or databases or both.

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

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

1.4.2 Understanding the Application Tier

The application tier is the tier where J2EE applications are deployed. Products such as Oracle Directory Integration Platform, Oracle Identity Federation, Oracle Directory Services Manager and Oracle Enterprise Manager Fusion Middleware Control are the key J2EE components that can be deployed in this tier. Applications in this tier benefit from the High Availability support of Oracle WebLogic Server.

The Identity Management applications in the application tier interact with the directory tier:

- In some cases, they leverage the directory tier for enterprise identity information.
- In some cases, they leverage the directory tier (and some times the database in the data tier) for application metadata.
- Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager are administration tools that provide administrative functionalities to the components in the application tier as well as the directory tier.
- WebLogic Server has built-in web server support. If enabled, the HTTP listener will exist in the application tier as well. However, for the enterprise deployment shown in Figure 1–1, customers will have a separate web tier relying on web servers such as Apache or Oracle HTTP Server.

In the application tier:

- IDMHOST1 and IDMHOST2 have the WebLogic Server with the Administration Console, Oracle Enterprise Manager Fusion Middleware Control, Oracle Directory Integration Platform, and Oracle Directory Services Manager installed.

  IDMHOST1 and IDMHOST2 run both the WebLogic Server Administration Servers and Managed Servers. Note that the administration server is configured to be active-passive, that is, although it is installed on both nodes, only one instance

is active at any time. If the active instance goes down, then the passive instance starts up and becomes the active instance.

- On the firewall protecting the application tier, the HTTP ports, NIP port, and NAP port are open. The NIP (Network Identity Protocol) port is for the WebPass module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as querying user groups. The NAP (Network Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.
- OAMHOST1 and OAMHOST2 have Oracle Access Manager (with the Identity Server and Access Server components) installed. Oracle Access Manager is the single sign-on component for Oracle Fusion Middleware. It communicates with Oracle Internet Directory in the directory tier to verify user information.
- OAMADMINHOST is on an isolated subnet (for Oracle Access Manager administration), and it has Oracle HTTP Server, WebGate, WebPass, and Policy Manager installed.

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server and Oracle Enterprise Manager are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.

High Availability Provisions

- Identity and Access servers are active-active deployments; the Access Server may communicate with the Identity Server at run time.
- The WebLogic Administration Server and Oracle Enterprise Manager deployment is active-passive (where other components are active-active).
- The WebLogic Administration Server is a singleton component deployed in an active-passive configuration. If IDMHOST1 fails or the Administration Server on IDMHOST1 does not start, the Administration Server on IDMHOST2 can be started. All Managed Servers and components on IDMHOST1 and IDMHOST2 must be configured with the Administration Server virtual IP.

Security Provisions

- WebPass communication from the public DMZ to Identity and Access Servers is not allowed.
- The Policy Manager (an Oracle HTTP Server module secured with both WebGate and WebPass) is deployed in an isolated administrative subnet, which communicates directly with Oracle Internet Directory.

1.4.3 Understanding the Web Tier

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

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

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

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the mod_wl_ohs plug-in module installed. The mod_wl_ohs plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Network Access Protocol (NAP) to communicate with Oracle Access Manager running on OAMHOST1 and OAMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.
- On the firewall protecting the web tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.

Architecture Notes

- Oracle HTTP Servers on WEBHOST1 and WEBHOST2 are configured with mod_wl_ohs, and proxy requests for the Oracle Enterprise Manager, Oracle Directory Integration Platform, and Oracle Directory Services Manager J2EE applications deployed in WebLogic Server on IDMHOST1 and IDMHOST2.

Security Provisions

- WebPass is installed on OAMADMINHOST along with the Policy Manager. The Policy Manager and the WebPass are used to configure the Access Servers and the Identity Servers on OAMHOST1 and OAMHOST2.
- WebGate is installed on OAMADMINHOST to protect the Policy Manager, and configured on WEBHOST1 and WEBHOST2 to protect inbound access.
- Oracle Access Manager Identity Assertion Provider for WebLogic Server 11*g*R1 is installed on IDMHOST1 and IDMHOST2.

1.4.4 What to Install

Table 1–2 identifies the source for installation of each software component:

Table 1–2 Components and Installation Sources

Component	CD
Oracle Database 10*g* or 11*g*	Oracle Database CD (10.2.0.4 or higher) Oracle Database CD (11.1.0.7)
Oracle WebLogic Server	WebLogic Server 10.3.1 CD
Oracle Identity and Access Management Components	This includes 11g Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Integration Platform, Oracle Directory Services Manager, Oracle Identity Federation, as well as Oracle Access Manager 10.1.4.3 components. Oracle Identity Management CD (11.1.1.1.0)
Repository Creation Utility	Oracle Fusion Middleware Repository Creation Utility CD (11.1.1.1.0)
Oracle HTTP Server	Oracle Fusion Middleware Web Tier and Utilities CD (11.1.1.1.0)

For information about the order in which to perform the installations, see Section 1.5, "How to Use This Guide."

1.5 How to Use This Guide

The chapters in the guide are arranged chronologically. Complete the procedures in the sections as shown in the table according to the desired configuration.

Step	Section
Read the introduction to the enterprise deployment	Section 1.1, "What is an Enterprise Deployment?"
Learn the new terminology associated with the enterprise deployment	Section 1.2, "Terminology"
Review the benefits of Oracle recommendations	Section 1.3, "Benefits of Oracle Recommendations"
See an overview of the enterprise deployment	Section 1.4, "The Enterprise Deployment Reference Topology"
View the hardware requirements	Section 2.1, "Hardware Resource Planning"
View the network prerequisites	Section 2.2, "Network Prerequisites"
Review the WebLogic domain considerations	Section 2.3, "WebLogic Domain Considerations"
Install Oracle WebLogic Server on IDMHOST1	Section 3.1, "Installing Oracle WebLogic Server"
Configure the Oracle WebLogic Server domain on IDMHOST1	Section 3.2, "Configuring the WebLogic Server Domain on IDMHOST1"
Creating boot.properties for the Administration Server	Section 3.3, "Creating boot.properties for the Administration Server"
Back up the WebLogic Server domain configuration	Section 3.4, "Backing Up the WebLogic Server Domain Configuration"
View the directory tier considerations	Section 4.1, "Directory Tier Considerations"
View the database prerequisites	Section 4.2, "Database Prerequisites"
Install and configure the Oracle database repository on INFRADBHOST1 and INFRADBHOST2	Section 4.3, "Installing and Configuring the Database Repository"

Step	Section
Run the Repository Creation Utility to create the Oracle Identity Management schemas in the database	Section 4.4, "Executing the Repository Creation Utility."
Install the Oracle Internet Directory instances on OIDHOST1 and OIDHOST2	Section 4.5, "Installing the Oracle Internet Directory Instances"
Install the Oracle Virtual Directory instances on OVDHOST1 and OVDHOST2	Section 4.6, "Installing the Oracle Virtual Directory Instances"
Validate the directory tier components	Section 4.7, "Validating the Directory Tier Components"
Back up the directory tier	Section 4.8, "Backing Up the Directory Tier Configuration"
Install and configure Oracle Directory Integration Platform and Oracle Directory Services Manager on IDMHOST1	Section 5.1, "Extending the Oracle WebLogic Domain with DIP and ODSM"
Expand the Oracle Directory Integration Platform and Oracle Directory Services Manager cluster	Section 5.2, "Expanding the DIP and ODSM Cluster"
Validate the application tier configuration	Section 5.3, "Validating the Application Tier Configuration"
Back up the application tier configuration	Section 5.4, "Backing Up the Application Tier Configuration"
View the web tier prerequisites	Section 6.1, "Prerequisites"
Install Oracle HTTP Server on WEBHOST1 and WEBHOST2	Section 6.2, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2"
Validate the Oracle HTTP Server installations	Section 6.3, "Validating the Installations of Oracle HTTP Server"
Configure Oracle HTTP Server with the load balancer	Section 6.4, "Configuring Oracle HTTP Server with the Load Balancer"
Configure Oracle HTTP Server with the virtual hosts	Section 6.5, "Configuring Oracle HTTP Server for Virtual Hosts"
Configure mod_wl_ohs for Oracle WebLogic Server clusters	Section 6.6, "Configuring mod_wl_ohs for Oracle WebLogic Server Clusters"
Set the frontend URL for the Oracle WebLogic Server Administration Console	Section 6.7, "Setting the Frontend URL for the Administration Console"
Validate the web tier configuration	Section 6.8, "Validating the Web Tier Configuration"
Back up the web tier configuration	Section 6.9, "Backing up the Web Tier Configuration"
Read the introduction to installing Oracle Access Manager	Section 7.1, "Introduction to Installing Oracle Access Manager"
Read the Oracle Access Manager prerequisites	Section 7.2, "Prerequisites"
Install and configure the Oracle Access Manager Identity System on OAMHOST1, OAMHOST2, and OAMADMINHOST	Section 7.3, "Identity System Installation and Configuration"

Step	Section
Install and configure the Oracle Access Manager Access System on OAMADMINHOST, OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2	Section 7.4, "Access System Installation and Configuration"
Back up the Oracle Access Manager configuration	Section 7.5, "Backing Up the Oracle Access Manager Configuration"
View the prerequisites for configuring Single Sign-On for administration consoles	Section 8.1, "Prerequisites for Configuring Single Sign-On"
Run the OAM configuration tool	Section 8.2, "Running the Oracle Access Manager Configuration Tool"
Validate the policy domain and AccessGate configurations	Section 8.3, "Validating the Policy Domain and AccessGate Configurations"
Set up the WebLogic authenticators	Section 8.4, "Setting Up the WebLogic Authenticators"
Change the Login form for the Administration Server	Section 8.5, "Changing the Login Form for the Administration Server"
Move the WebLogic administrator to LDAP	Section 8.6, "Creating WebLogic Administrative Users in an LDAP Directory"
Migrate the policy and credential store	Section 8.7, "Policy and Credential Store Migration"
Validate the Oracle Access Manager Single Sign-On setup	Section 8.8, "Validate the Oracle Access Manager Single Sign-On Setup"
Configure the WebLogic Administration Server	Section 9.1, "Configuring High Availability for Oracle WebLogic Administration Server"
Provision the Administration Server and Oracle Fusion Middleware Control on IDMHOST2	Section 9.2, "Provisioning the Administration Server and Fusion Middleware Control on IDMHOST2"
Validate Administration Server and Oracle Enterprise Manager Fusion Middleware Control failover	Section 9.3, "Validating Administration Server and Oracle Fusion Middleware Control Failover on IDMHOST2"
Monitor the enterprise deployment	Section 10.1, "Monitoring Enterprise Deployments"
Audit the enterprise deployment	Section 10.2, "Auditing Identity Management"
Scale the enterprise deployment	Section 10.3, "Scaling Enterprise Deployments"
Back up and recover the enterprise deployment	Section 10.4, "Performing Backups and Recoveries"
Patch the enterprise deployment	Section 10.5, "Patching Enterprise Deployments"
Troubleshoot the enterprise deployment	Section 10.6, "Troubleshooting"
Best practices for the enterprise deployment	Section 10.7, "Other Recommendations"

2

Prerequisites for Enterprise Deployments

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

This chapter includes the following topics:

- Section 2.1, "Hardware Resource Planning"
- Section 2.2, "Network Prerequisites"
- Section 2.3, "WebLogic Domain Considerations"

2.1 Hardware Resource Planning

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

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

Table 2–1 Typical Hardware Requirements

Server	Processor	Disk	Memory	TMP Directory	Swap
INFRADBHOSTn	4 or more X Pentium 1.5 GHz or greater	nXm n=Number of disks, at least 4 (striped as one disk). m=Size of the disk (minimum of 30 GB)	6-16 GB	Default	Default
WEBHOSTn	4 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default
IDMHOSTn, OAMHOSTn	4 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default
OAMADMINHOST	4 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default
OIDHOSTn, OVDHOSTn	4 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default

These are the typical hardware requirements. For each tier, carefully consider the load, throughput, response time and other requirements to plan the actual capacity required. The number of nodes, CPUs, and memory required can vary for each tier

based on the deployment profile.Production requirements may vary depending on applications and the number of users.

The Enterprise Deployment configurations described in this guide use two servers for each tier to provide failover capability; however, this does not presume adequate computing resources for any application or user population. If the system workload increases such that performance is degraded, you can add servers to the configuration by repeating the instructions for the second server (that is, WEBHOST2, IDMHOST2, OIDHOST2, OVDHOST2, INFRADBHOST2) to install and configure additional servers where needed.

2.2 Network Prerequisites

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

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

2.2.1 Load Balancers

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
- Monitoring of ports (HTTP and HTTPS)
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
  - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for OracleAS Clusters, the load balancer 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.
- Resource monitoring / port monitoring / process failure detection: The load balancer must be able to detect service and node failures (through notification or some other means) and to stop directing non-Oracle Net traffic to the failed node.

If your external load balancer has the ability to automatically detect failures, you should use it.

- Fault tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- Other: It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the 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 based on cookies or URL.
- SSL acceleration (this feature is recommended, but not required)
- Configure the virtual server(s) in the load balancer for the directory tier with a high value for the connection timeout for TCP connections. This value should be more than the maximum expected time over which no traffic is expected between the Oracle Access Manager and the directory tier.

2.2.2 Configuring Virtual Server Names and Ports on the Load Balancer

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

There are two load balancer devices in the recommended topology. One load balancer is set up for external HTTP traffic and the other load balancer is set up for internal LDAP traffic. A deployment may choose to have a single load balancer device due to a variety of reasons. While this is supported, the deployment should consider the security implications of doing this and if found appropriate, open up the relevant firewall ports to allow traffic across the various DMZs. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant mode. The rest of this document assumes that the deployment is the one shown in Figure 1–1.

oid.mycompany.com

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

Note: Oracle recommends that you configure the same port for SSL connections on the LDAP server and Oracle Internet Directory on the computers on which Oracle Internet Directory is installed.

This is a requirement for most Oracle 10*g* products that need to use Oracle Internet Directory via the load balancing router.

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

ovd.mycompany.com

- This virtual server is enabled on `LBR2`. It acts as the access point for all LDAP traffic to the Oracle Virtual Directory servers in the directory tier. Traffic to both the SSL and non-SSL is configured. The clients access this service using the address `ovd.mycompany.com:636` for SSL and `ovd.mycompany.com:389` for non-SSL.
- Monitor the heartbeat of the Oracle Virtual Directory processes on OVDHOST1 and OVDHOST2. If an Oracle Virtual Directory process stops on OVDHOST1 or OVDHOST2, or if either host OVDHOST1 or OVDHOST2 is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

admin.mycompany.com

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

sso.mycompany.com

- This virtual server is enabled on `LBR1`. It acts as the access point for all HTTP traffic that gets directed to the single sign on services. The incoming traffic from clients is SSL enabled. Thus, the clients access this service using the address `sso.mycompany.com:443` and in turn forward these to ports 7777 on WEBHOST1 and WEBHOST2. All the single sign on enabled protected resources are accessed on this virtual host.
- Create rules in the firewall to block outside traffic from accessing the `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `admin.mycompany.com` virtual host.
- Configure this virtual server in the load balancer with both port 80 and port 443. Any request that goes to port 80 must be redirected to port 443 in the load balancer.

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

2.2.3 Administration Server Virtual IP

idmhost-vip.mycompany.com

A virtual IP 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 will be configured later to listen on this virtual IP address, as discussed later in this manual. The virtual IP address fails over along with the Administration Server from IDMHOST1 to IDMSHOST2, or vice versa.

2.2.4 Managing Oracle Fusion Middleware Component Connections

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

2.2.5 Oracle Access Manager Communication Protocol and Terminology

Oracle Access Manager components use proprietary protocols called Oracle Access Protocol (OAP) and Oracle Identity Protocol (OIP) to communicate with each other.

2.2.5.1 Oracle Access Manager Protocols

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

Oracle Identity Protocol (OIP) governs communications between Identity System components (for example, Identity Server, WebPass) and a Web server. This protocol was formerly known as NetPoint Identity Protocol (NIP) or COREid Identity Protocol).

2.2.5.2 Overview of User Request

The request flow when a user requests access is described below:

1. The user requests access to a protected resource over HTTP or HTTPS.
2. The WebGate intercepts the request.
3. The WebGate forwards the request to the Access Server over Oracle Access Protocol to determine if the resource is protected, how, and whether the user is authenticated (if not, there is a challenge).
4. The Access Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate over Oracle Access Protocol, and generates an encrypted cookie to authenticate the user.
5. Following authentication, the WebGate prompts the Access Server over Oracle Access Protocol and the Access Server looks up the appropriate security policies, compares them to the user's identity, and determines the user's level of authorization.
   - If the access policy is valid, the user is allowed to access the desired content and/or applications.
   - If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

2.2.6 Firewall and Port Configuration

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

Most port numbers are assigned during installation.

Table 2–2 lists the ports used in the Oracle Identity Management topology, including the ports that you need to 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 directory tier.

Table 2–2 Ports Used in the Oracle Identity 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 Management.
Browser request	FW0	443	HTTPS / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity Management.
Oracle WebLogic Administration Server access from web tier	FW1	7001	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Enterprise Manager Agent - web tier to Enterprise Manager	FW1	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
Oracle HTTP Server to WLS_ODS	FW1	7006	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the mod_ weblogic parameters used.
Oracle Process Manager and Notification Server (OPMN) access in web tier	FW1	OPMN remote port	HTTP / Administration Server to OPMN	Outbound	N/A
Oracle HTTP Server proxy port	FW1	9999	HTTP / Administration Server to Oracle HTTP Server	Outbound	N/A
Access Server access	FW1	6021	NAP	Both	N/A
Oracle WebLogic Administration Server access from directory tier	FW2	7001	HTTP / Oracle Internet Directory, Oracle Virtual Directory, and Administration Server	Outbound	N/A
Enterprise Manager Agent - directory tier to Enterprise Manager	FW2	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
OPMN access in directory tier	FW2	OPMN remote port	HTTP / Administration Server to OPMN	Inbound	N/A

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

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Oracle Virtual Directory proxy port	FW2	8899	HTTP / Administration Server to Oracle Virtual Directory	Inbound	N/A
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Identity Management.
Oracle Internet Directory access	FW2	389	LDAP	Inbound	You should tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Internet Directory access	FW2	636	LDAP SSL	Inbound	You should tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	6501	LDAP	Inbound	Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	7501	LDAP SSL	Inbound	Ideally, these connections should be configured not to time out.
Load balancer to Oracle HTTP Server	N/A	7777	HTTP	N/A	N/A
Session replication within a WebLogic Server cluster	N/A	N/A	N/A	N/A	By default, this communication uses the same port as the server's listen address.
Node Manager	N/A	5556	TCP/IP	N/A	N/A
WebGate access from OAMADMINHOST	N/A	This is optional. You can use the listen port of the Oracle HTTP Server where the WebGate is configured (7777)	NAP	N/A	N/A
WebPass access from OAMADMINHOST	N/A	6022	NIP	N/A	N/A
Identity Server access	N/A	6022	NIP	N/A	N/A

2.3 WebLogic Domain Considerations

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

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

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

2.3.1 Directory Structure Terminology and Recommendations

This section provides directory structure terminology and recommendations for the enterprise deployment.

2.3.1.1 Directory Structure Terminology

This section describes directory structure terminology and environment variables.

- ORACLE_BASE: This environment variable and related directory path refers to the base directory under which Oracle products are installed.
- MW_HOME: This environment variable and related directory path refers to the location where Oracle Fusion Middleware resides.
- WL_HOME: This environment variable and related directory path contains installed files necessary to host a WebLogic Server.
- ORACLE_HOME: This environment variable and related directory path refers to the location where Oracle Fusion Middleware Identity Management is installed.
- DOMAIN directory: This directory path refers to the location where the Oracle WebLogic domain information (configuration artifacts) is stored. Different WebLogic Servers can use different domain directories even when in the same node as described Section 2.3.1.2, "Directory Structure Recommendations."
- ORACLE_INSTANCE: An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. An Oracle instance directory contains updateable files, such as configuration files, log files, and temporary files.

2.3.1.2 Directory Structure Recommendations

Oracle Fusion Middleware 11*g* allows the separation of the product binaries and the runtime artifacts. The product binaries are under the *ORACLE_HOME* directory and the runtime time artifacts are located under the *ORACLE_INSTANCE* directory.

In this enterprise deployment model, for the web tier and the data tier, it is recommended to have one ORACLE_HOME (for product binaries) per host and one

ORACLE_INSTANCE for an instance, installed on the local disk. The ORACLE_HOME is shared among all the instances running on the host, whereas each instance has its own ORACLE_INSTANCE location. Additional, servers (when scaling out or up) of the same type can use either one of the same location without requiring more installations.

For the application tier, it is recommended to have one Middleware Home (MW HOME) per host (each of which has a WLS HOME and an ORACLE_HOME for each product suite) installed on the local disk. Additional servers (when scaling out or up) of the same type can use the same location without requiring more installations.

Separation of the domain directory and the MW_HOME is not supported. The domain directory is under the MW_HOME and is shared between all the Administration Servers and Managed Servers running on the host.

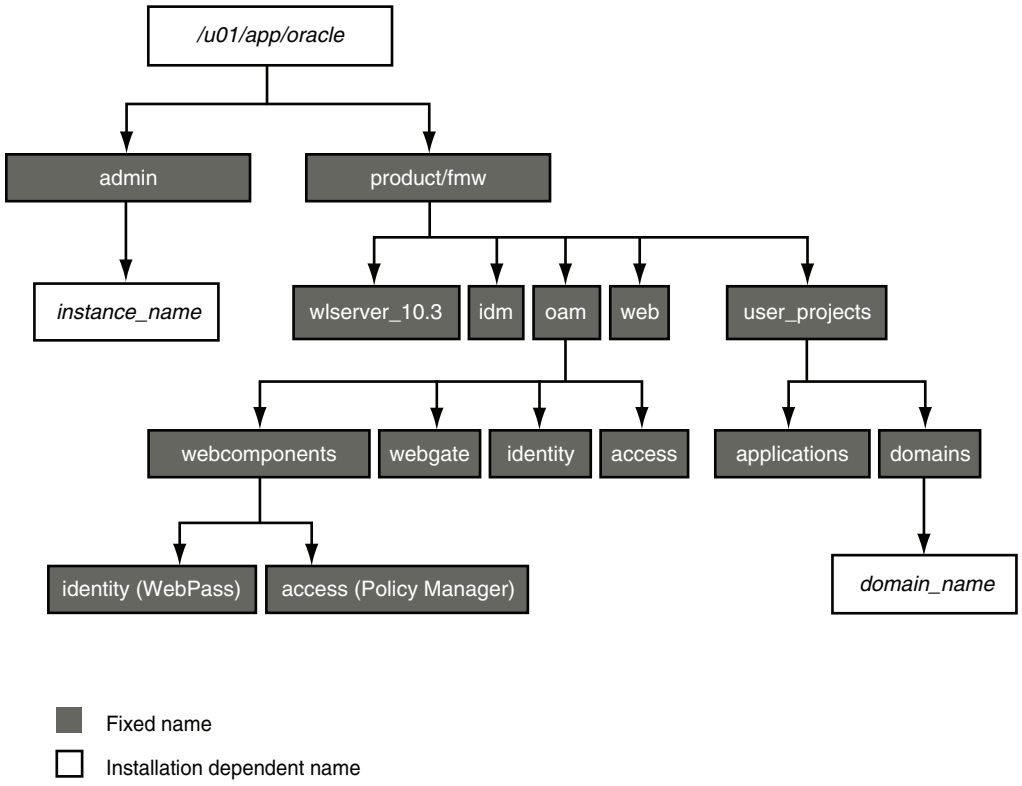
Based on the above recommendations, Table 2–3 lists the recommended directory structure. The directory locations listed are examples and can be changed. However, Oracle recommends that these locations be used for uniformity, consistency and simplicity.

Table 2–3 Directory Structure for Enterprise Deployment

Tier	Parameter/Values
Common	*ORACLE_BASE*=/u01/app/oracle
	MW_HOME=ORACLE_BASE/product/fmw
	ORACLE_INSTANCE=ORACLE_BASE/admin/*instanceName*
Web Tier	*ORACLE_HOME=MW_HOME*/web
Application Tier	*ORACLE_HOME =MW_HOME*/idm
	DOMAIN_HOME=MW_HOME/user_projects/domains/*domainName*
	APPLICATIONS_HOME=MW_HOME/user_projects/applications
Oracle Access Manager	*OAM_BASE=MW_HOME*/oam
	I*DENTITY_SERVER_ORACLE_HOME=OAM_BASE*/identity
	ACCESS_SERVER_ORACLE_HOME=OAM_BASE/access
	WEBPASS_ORACLE_HOME=OAM_BASE/webcomponents/identity
	POLICY_MANAGER_ORACLE_HOME=OAM_BASE/webcomponents/access
	WEBGATE_ORACLE_HOME=OAM_BASE/webgate
Data Tier	*ORACLE_HOME=MW_HOME*/idm

Figure 2–1 shows the recommended directory structure.

Figure 2–1 Oracle Home Directories for Components in This Manual



3

Creating the WebLogic Server Domain for Identity Management

This chapter describes how to create the WebLogic Server domain for Identity Management.

This chapter includes the following topics:

3.1 Installing Oracle WebLogic Server

On IDMHOST1 and IDMHOST2, start the Oracle WebLogic Server installation by running the installer executable file.

Start the Oracle WebLogic Server installer as follows:

- On Linux, issue this command:

```
./server103_linux32.bin
```

Then follow these steps in the installer to install Oracle WebLogic Server on the computer:

1. On the Welcome screen, click **Next**.
2. On the Choose Middleware Home Directory screen, choose a directory on your computer into which the Oracle WebLogic software is to be installed.

   For the **Middleware Home Directory**, specify this value:

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

   Click **Next**.
3. On the Register for Security Updates screen, enter your "My Oracle Support" UserName and Password.
4. On the Choose Install Type screen, the installation program displays a window in which you are prompted to indicate whether you wish to perform a complete or a custom installation.

   Choose **Typical.**

   Click **Next**.

5. On the Choose Product Installation Directories screen, specify the following value:

   WebLogic Server:

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

   Click **Next**.

6. On the Installation Summary screen, the window contains a list of the components you selected for installation, along with the approximate amount of disk space to be used by the selected components once installation is complete.

   Click **Next**.

7. On the Installation Complete screen deselect the **Run Quickstart** checkbox and then click **Done**.

3.2 Configuring the WebLogic Server Domain on IDMHOST1

Follow these steps to configure the WebLogic Server domain on IDMHOST1:

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

2. Ensure that port numbers 7001 and 5556 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "7001"
   netstat -an | grep "5556"
   ```

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

   On UNIX:

   Remove the entries for ports 7001 and 5556 in the `/etc/services` file if the port is in use by a service and restart the services, or restart the computer.

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

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

   Domain Port No: `7001`

   Node Manager Port No: 5556

5. Start the Oracle Identity Management 11g Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   This displays the Specify Oracle Inventory screen.

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

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

Operating System Group Name: `oinstall`

A dialog box appears with the following message:

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

Login as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

---

7. On the Welcome screen, click **Next**.
8. On the Select Installation Type screen, select the **Install & Configure Option**, and then click **Next**.
9. On the Prerequisite Checks screen, the installer completes the prerequisite check. If any fail, please fix them and restart your installation.
10. On the Select Domain screen, select **Create New Domain**.

    Then enter these values for these fields:

    User Name: `weblogic`

    User Password: `<Enter the user password>`

    Confirm Password: `<Confirm the user password>`

    Domain Name: `IDMDomain`
11. On the Specify Installation Locations screen, specify the following values:

    Oracle Middleware Home Location:

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

    Oracle Home Directory: idm

    WebLogic Server Directory:

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

    Oracle Instance Location:

    `/u01/app/oracle/admin/admin_inst`

    Oracle Instance Name: `admin_inst`
12. On the Specify Email for Security Updates screen, specify these values:

- **Email Address**: Provide the email address for your My Oracle Support account.
- **Oracle Support Password**: Provide the password for your My Oracle Support account.
- Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

13. On the Configure Components screen, de-select everything except Enterprise Manager (this is selected by default)
14. On the Configure Ports screen, select **Specify Ports using Configuration file - Path to staticports.ini file** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.
15. On the Installation Summary screen, review the choices you made. If you need to make any changes click **Back**. If you made the correct selections, click **Install**.
16. On the Installation Progress screen, view the progress of the installation.

    Once the installation is done, the oracleRoot.sh confirmation dialog box displays. This dialog box advises you that a configuration script needs to be run as root before installation can proceed.

    Leaving this dialog box open, open another shell window, log in as root, and run the oracleRoot.sh file specified in the dialog box.
17. On the Configuration Progress screen, view the progress of the configuration.
18. On the Installation Complete screen, click **Finish**.
19. Validate that the domain was created and installed correctly by opening a web browser and accessing the following pages:

    WebLogic Server Administration Console at:

    `http://idmhost1.mycompany.com:7001/console`

    Oracle Enterprise Manager Fusion Middleware Control at:

    `http://idmhost1.mycompany.com:7001/em`

    Log into these consoles using the `weblogic` user credentials.

3.3 Creating boot.properties for the Administration Server

This section describes how to create a `boot.properties` file for the Administration Server on IDMHOST1. The `boot.properties` file enables the Administration Server to start without prompting for the administrator username and password.

Follow these steps to create the `boot.properties` file:

1. On IDMHOST1, go the *`MW_HOME`*`/user_projects/domains/`*`domainName`*`/servers/AdminServer/security` directory. For example:

   ```
   cd /u01/app/oracle/product/fmw/user_
   projects/domains/IDMDomain/servers/AdminServer/security/
   ```

2. 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
```

> **Note:** When you start the Administration Server, the username and password entries in the file get encrypted.
>
> For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

3. Stop the Administration Server if it is running.

   See the "Starting and Stopping Oracle Fusion Middleware" chapter of the *Oracle Fusion Middleware Administrator's Guide* for information on starting and stopping WebLogic Servers.

4. Start the Administration Server on IDMHOST1 using the `startWebLogic.sh` script located under the *`MW_HOME`*`/user_projects/domains/`*`domainName`*`/bin` directory.

5. Validate that the changes made were successful by opening a web browser and accessing the following pages:

   - WebLogic Server Administration Console at:

     `http://idmhost1.mycompany.com:7001/console`

   - Oracle Enterprise Manager Fusion Middleware Control at:

     `http://idmhost1.mycompany.com:7001/em`

   Log into these consoles using the `weblogic` user credentials.

3.4 Backing Up the WebLogic Server Domain Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restore in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

To back up the installation to this point, back up the Administration Server domain directory. All the configuration files exist under the *`MW_HOME`*`/user_projects/domains/`*`domainName`* directory. To create a backup to save your domain configuration, use the `tar` command as shown below:

```
IDMHOST1> tar cvf edgdomainback.tar MW_HOME/user_projects/domains/domainName
```

For more information about backing up the Oracle WebLogic Server domain configuration, see Section 10.4, "Performing Backups and Recoveries."

4

Installing and Configuring OID and OVD

This chapter describes how to install and configure Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) in the enterprise deployment.

This chapter includes the following topics:

4.1 Directory Tier Considerations

Using these naming conventions will simplify the installation and maintenance of the enterprise deployment:

- Use the same path for the Oracle home directory. For all the nodes that will be running Oracle Identity Management components, use the same full path for the Oracle home.
- Table 4–1 shows the names used in database configuration examples in this guide:

Table 4–1 Values Used for Database Configuration Examples in This Manual

Parameter	Value
DB_NAME	idmdb
INSTANCE_NAMES	idmdb1, idmdb2
SERVICE_NAME	idmedg.mycompany.com

4.1.1 Directory Services-only Topologies

The topology shown in Figure 1–1 and discussed in this document represents a common deployment. However, customers may have different topology requirements. In some cases, only a subset of the components is needed. In other cases, certain components can be replaced by others.

Some customers may be interested in only deploying a directory services topology. See the following sections for more information about an Oracle Virtual Directory-only topology and an Oracle Internet Directory-only topology.

4.1.1.1 Oracle Virtual Directory-only Topology

For an Oracle Virtual Directory-only topology, do not install Oracle Internet Directory in the directory tier. Because Oracle Virtual Directory relies on Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager, the Administration Server for Oracle Enterprise manager and the WebLogic Server Managed Server for Oracle Directory Services Manager are required.

4.1.1.2 Oracle Internet Directory-only Topology

For an Oracle Internet Directory-only deployment, you can choose to deploy Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager by deploying the corresponding Administration Server and WebLogic Server Managed Server, respectively. This will create a WebLogic Server domain as the administrative domain for the Oracle Internet Directory instances.

For Oracle Internet Directory, the installer also offers a no-domain installation, meaning that a WebLogic Server domain will not be created. As a result, a no-domain Oracle Internet Directory installation will result in Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager not being deployed. The type of deployment is for customers who are familiar with managing Oracle Internet Directory through the command line and through LDAP commands. This deployment provides a leaner footprint for those interested in having just a LDAP server without the administration consoles.

For those interested in having Oracle Directory Integration Platform as an LDAP synchronization solution, the administration console should be deployed. The WebLogic Server Managed Server will be used for the Oracle Directory Integration Platform J2EE application as shown in the EDG topology in Figure 1–1.

4.2 Database Prerequisites

Before you begin to install and configure the directory tier components, you must perform these steps:

- Install and configure the Oracle database repository.

  This step is described in Section 4.3, "Installing and Configuring the Database Repository."

- Create the Oracle Identity Management schemas in the database using the Repository Creation Utility (RCU).

  This step is described in Section 4.4, "Executing the Repository Creation Utility."

Database versions supported

- Oracle Database 10g Release 2 (10.2.0.4 or higher)
- Oracle Database 11g Release 1 (11.1.0.7 or higher)

To determine the database version, execute this query:

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

4.3 Installing and Configuring the Database Repository

Oracle Clusterware

- For 10*g* Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide*.
- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide*.
- For 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** page to create a separate Automatic Storage Management home.

Oracle Real Application Clusters

- For 10*g* Release 2 (10.2), see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide*.
- For 11*g* Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

4.3.1 Configuring the Database for Oracle Fusion Middleware 11g Metadata

Initialization Parameters

Update the following utilization parameters to the values shown below. These values are checked by the Repository Creation Utility (RCU). If these initialization parameters are not set to the values shown below, RCU will fail:

- `processes`: 500
- `open_cursors`: 500
- `session_cached_cursors`: 100

The value of the static initialization parameter `processes` must be 500 or greater for Oracle Internet Directory. This value is checked by the Repository Creation Utility.

To check the value, you can use the `SHOW PARAMETER` command in SQL*Plus:

```
prompt> sqlplus "sys/password as sysdba"
SQL> SHOW PARAMETER processes
```

One common method of changing the parameter value is to use a command similar to the following and then stop and restart the database to make the parameter take effect:

```
prompt> sqlplus "sys/password as sysdba"
SQL> ALTER SYSTEM SET PROCESSES=500 SCOPE=SPFILE;
```

The method that you use to change a parameter's value depends on whether the parameter is static or dynamic, and on whether your database uses a parameter file or a server parameter file. See the *Oracle Database Administrator's Guide* for details on parameter files, server parameter files, and how to change parameter values.

Database Services

Oracle recommends using the Oracle Enterprise Manager Cluster Managed Services Page to create database services that client applications will use to connect to the database. For complete instructions on creating database services, see the chapter on Workload Management in the *Oracle Real Application Clusters Administration and Deployment Guide*.

You can also use SQL*Plus to configure your RAC database to automate failover for Oracle Internet Directory using the following instructions. Note that each of the following commands only has to be run on one node in the cluster:

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

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

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

   The EXECUTE DBMS_SERVICE command above must be entered on a single line to execute properly.

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

   ```
   prompt> srvctl add service -d idmdb -s idmedg -r idmdb1,idmdb2
   ```

3. Start the service using srvctl:

   ```
   prompt> srvctl start service -d idmdb -s  idmedg
   ```

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

If you already have a service created in the database, make sure that it is enabled for high-availability notifications and configured with the proper server-side Transparent Application Failover (TAF) settings. Use the DBMS_SERVICE package to modify the service to enable high availability notification to be sent through Advanced Queuing (AQ) by setting the AQ_HA_NOTIFICATIONS attribute to TRUE and configure server-side Transparent Application Failover (TAF) settings, as shown below:

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

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

The EXECUTE DBMS_SERVICE command above must be entered on a single line to execute properly.

Note: For more information about the DBMS_SERVICE package, see the *Oracle Database PL/SQL Packages and Types Reference*.

Verifying Transparent Application Failover

This section describes how to validate the Transparent Application Failover (TAF) configuration settings made earlier.

After the Oracle Internet Directory process has been started, you can query the FAILOVER_TYPE, FAILOVER_METHOD, and FAILED_OVER columns in the V$SESSION_VIEW to obtain information about connected clients and their TAF status.

For example, use the following SQL statement to verify that TAF is correctly configured:

```
SELECT MACHINE, FAILOVER_TYPE, FAILOVER_METHOD, FAILED_OVER, COUNT(*)
FROM V$SESSION
GROUP BY MACHINE, FAILOVER_TYPE, FAILOVER_METHOD, FAILED_OVER;
```

The output before failover is similar to this:

```
MACHINE              FAILOVER_TYPE FAILOVER_M  FAI   COUNT(*)
-------------------- ------------- ---------- ---- ----------
oidhost1             SELECT        BASIC      NO           11
oidhost1             SELECT        BASIC      NO            1
```

The output after failover is similar to this:

```
MACHINE              FAILOVER_TYPE FAILOVER_M  FAI   COUNT(*)
-------------------- ------------- ---------- ---- ----------
oidhost2             SELECT        BASIC      NO           11
oidhost2             SELECT        BASIC      NO            1
```

4.4 Executing the Repository Creation Utility

The Repository Creation Utility (RCU) ships on its own CD as part of the Oracle Fusion Middleware 11*g* kit.

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

1. Issue this command:

   ```
   prompt> RCU_HOME/bin/rcu &
   ```

2. On the Welcome screen, click **Next**.
3. On the Create Repository screen, select the **Create** operation to load component schemas into an existing database. Then click **Next**.
4. On the Database Connection Details screen, enter connection information for the existing database as follows:

   Database Type: `Oracle Database`

   Host Name: Name of the computer on which the database is running. For a RAC Database, specify the VIP name or one node name. Example: `INFRADBHOST1-VIP` or `INFRADBHOST2-VIP`

   Port: The port number for the database. Example: `1521`

Service Name: The service name of the database. Example: `idmedg.mycompany.com`

Username: `SYS`

Password: The SYS user password

Role: `SYSDBA`

Click **Next**.

5. On the Select Components screen, create a new prefix and select the components to be associated with this deployment:

   Create a New Prefix: `edgidm` (Entering a prefix is optional if you select only **Identity Management** (Oracle Internet Directory - ODS) in the **Components** field)

   Components: Select **Identity Management** (Oracle Internet Directory - ODS). De-select all other schemas.

   Click **Next**.

6. On the Schema Passwords screen, enter the passwords for the main and additional (auxiliary) schema users and click **Next**.
7. On the Map Tablespaces screen, select the tablespaces for the components.
8. On the Summary screen, click **Create**.
9. On the Completion Summary screen, click **Close**.

4.5 Installing the Oracle Internet Directory Instances

This section describes how to install the Oracle Internet Directory components (OIDHOST1 and OIDHOST2) on the directory tier with the Metadata Repository. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

4.5.1 Synchronizing the Time on Oracle Internet Directory Nodes

Before setting up Oracle Internet Directory in a high availability environment, you must ensure that the time on the individual Oracle Internet Directory nodes is synchronized.

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

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

4.5.2 Installing the First Oracle Internet Directory

Follow these steps to install the 11.1.1.1.0 Oracle Internet Directory on OIDHOST1:

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

2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

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

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

   On UNIX:

   Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.

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

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

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

5. Start the Oracle Identity Management 11*g* Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.

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

   - **Specify the Inventory Directory**: `/u01/app/oraInventory`
   - **Operating System Group Name**: `oinstall`

     A dialog box appears with the following message:

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

     Log in as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

---

7. On the Welcome screen, click **Next**.
8. On the Select Installation Type screen, select **Install and Configure** and then click **Next**.
9. On the Prerequisite Checks screen, the installer completes the prerequisite check. If any fail, please fix them and restart your Installation.

   Click **Next**.
10. On the Select Domain screen, select **Configure without a Domain**.

    Click **Next**.
11. On the Specify Installation Location screen, specify the following values:
    - **Oracle Home Location:**

      `/u01/app/oracle/product/fmw/idm`
    - **Oracle Instance Location**:

      `/u01/app/oracle/admin/oid_inst1`
    - **Oracle Instance Name**: oid_inst1

    Note: Ensure that the Oracle Home Location directory path for OIDHOST1 is the same as the Oracle Home Location path for OIDHOST2. For example, if the Oracle Home Location directory path for OIDHOST1 is:

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

    then the Oracle Home Location directory path for OIDHOST2 must be:

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

    Click **Next**.
12. On the Specify Email for Security Updates screen, specify these values:
    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

13. On the Configure Components screen, select **Oracle Internet Directory**, deselect all the other components, and then click **Next**.
14. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.

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

    - Connect String:

      ```
      infradbhost1-vip.mycompany.com:1521:idmdb1^infradbhost2-vip.mycompany.com:1
      521:idmdb2@idmedg.mycompany.com
      ```

      Note: The RAC database connect string information needs to be provided in the format *host1*:*port1*:*instance1*^*host2*:*port2*:*instance2*@*servicename*.

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

      It is required that the information provided above is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each RAC instance, and the service name provided must be configured for all the specified RAC instances.

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

    - User Name: `ODS`
    - Password: `******`

    Click **Next**.
16. On the Configure OID screen, specify the Realm and enter the Administrator (`cn=orcladmin`) password and click **Next**.
17. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
18. On the Installation Progress screen on UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window.

    Click **OK**.
19. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait for the configuration process to finish.
20. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
21. To validate the installation of the Oracle Internet Directory instance on OIDHOST1, issue these commands:

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

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

Note: See the "Configuring Your Environment" section of *Oracle Fusion Middleware User Reference for Oracle Identity Management* for a list of the environment variables you must set before using the `ldapbind` command.

4.5.3 Installing an Additional Oracle Internet Directory

The schema database must be running before you perform this task. Follow these steps to install the 11.1.1.1.0 Oracle Internet Directory on OIDHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

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

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

   On UNIX:

   Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.
3. Copy the `staticports.ini` file from the Disk1/stage/Response directory to a temporary directory.
4. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom ports:

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

5. Start the Oracle Identity Management 11*g* Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.
6. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
   - **Specify the Inventory Directory**: `/u01/app/oraInventory`
   - **Operating System Group Name**: `oinstall`

     A dialog box appears with the following message:

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

Log in as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

---

7. On the Welcome screen, click **Next**.
8. On the Select Installation Type screen, select **Install and Configure** and then click **Next**.
9. On the Prerequisite Checks screen, the installer completes the prerequisite check. If any fail, please fix them and restart your installation.

   Click **Next**.
10. On the Select Domain screen, select **Configure without a Domain**.

    Click **Next**.
11. On the Specify Installation Location screen, specify the following values:
    - **Oracle Home Location:**

      `/u01/app/oracle/product/fmw/idm`
    - **Oracle Instance Location**:

      `/u01/app/oracle/admin/oid_inst2`
    - **Oracle Instance Name**: oid_inst2

Note: Ensure that the Oracle Home Location directory path for OIDHOST1 is the same as the Oracle Home Location path for OIDHOST2. For example, if the Oracle Home Location directory path for OIDHOST1 is:

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

then the Oracle Home Location directory path for OIDHOST2 must be:

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

Click **Next**.

12. On the Specify Email for Security Updates screen, specify these values:
    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.

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

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

    Click **Next**.

15. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
    - Connect String:

      ```
      infradbhost1-vip.mycompany.com:1521:idmdb1^infradbhost2-vip.mycompany.com:1
      521:idmdb2@idmedg.mycompany.com
      ```

      Note: The RAC database connect string information needs to be provided in the format *host1*:*port1*:*instance1*^*host2*:*port2*:*instance2*@*servicename*.

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

      It is required that the information provided above is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each RAC instance, and the service name provided must be configured for all the specified RAC instances.

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

    - User Name: `ODS`
    - Password: `******`

    Click **Next**.

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

    Choose **Yes** to continue.

    A popup window with this message appears:

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

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

Click **OK** to continue.

17. On the Specify OID Admin Password screen, specify the OID Admin password and click **Next**.
18. 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**.
19. On the Installation Progress screen on UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window.

    Click **OK**.
20. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait for the configuration process to finish.
21. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
22. To validate the installation of the Oracle Internet Directory instance on OIDHOST2, issue these commands:

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

Note: See the "Configuring Your Environment" section of *Oracle Fusion Middleware User Reference for Oracle Identity Management* for a list of the environment variables you must set before using the `ldapbind` command.

4.5.4 Registering Oracle Internet Directory with the WebLogic Server Domain

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

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

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

```
export ORACLE_HOME=/u01/app/oracle/product/fmw/idm
```

2. Set the ORACLE_INSTANCE variable. For example:

On OIDHOST1, issue this command:

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

On OIDHOST2, issue this command:

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

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

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

For example, on OIDHOST1 and OIDHOST2:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost idmhost1.mycompany.com
-adminPort 7001 -adminUsername weblogic

Command requires login to weblogic admin server (idmhost1.mycompany.com)
 Username: weblogic
 Password: *******
```

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

4.6 Installing the Oracle Virtual Directory Instances

Follow these steps to install the Oracle Virtual Directory components (OVDHOST1 and OVDHOST2) on the directory tier with Oracle Internet Directory. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

4.6.1 Installing the First Oracle Virtual Directory

Follow these steps to install the Release 11*g* Oracle Virtual Directory on OVDHOST1.

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

```
netstat -an | grep "6501"
netstat -an | grep "7501"
```

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

   On UNIX:

Remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, or restart the computer.

4. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
5. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom ports:

```
# The non-SSL port for Oracle Virtual Directory
Oracle Virtual Directory port = 6501
# The SSL port for Oracle Virtual Directory
Oracle Virtual Directory (SSL) port = 7501
```

6. Start the Oracle Identity Management 11*g* Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.

7. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
   - **Specify the Inventory Directory**: `/u01/app/oraInventory`
   - **Operating System Group Name**: `oinstall`

     A dialog box appears with the following message:

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

     Log in as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

---

8. On the Welcome screen, click **Next**.
9. On the Select Installation Type screen, select **Install and Configure** and then click **Next**.
10. On the Prerequisite Checks screen, the installer completes the prerequisites check. If any fail, please fix them and restart your installation.

    Click **Next**.

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

    Click **Next**.

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

    - **Oracle Home Location:**

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

    - **Oracle Instance Location:**

      `/u01/app/oracle/admin/ovd_inst1`

    - **Oracle Instance Name**:

      `ovd_inst1`

    Note: Ensure that the Oracle Home Location directory path for OVDHOST1 is the same as the Oracle Home Location directory path for OVDHOST2. For example, if the Oracle Home Location directory path for OVDHOST1 is:

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

    then the Oracle Home Location directory path for OVDHOST2 must be:

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

    Click **Next**.

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

    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.

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

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

    Click **Next**.

16. On the Specify Virtual Directory screen:

    In the Client Listeners section, enter:

    - LDAP v3 Name Space:

      `dc=us,dc=mycompany,dc=com`

    In the OVD Administrator section, enter:

    - Administrator User Name: `cn=orcladmin`

- Password: `*******`
- Confirm Password: `*******`

Select **Configure the Administrative Server in secure mode**.

Click **Next**.

17. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
18. On the Installation Progress screen on UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window.

    Click **Next**.
19. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait for the configuration process to finish.
20. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
21. To validate the installation of the Oracle Virtual Directory instance on OVDHOST1, issue this command:

```
ldapbind -h ovdhost1.mycompany.com -p 6501 -D "cn=orcladmin" -q
```

> **Note:** See the "Configuring Your Environment" section of *Oracle Fusion Middleware User Reference for Oracle Identity Management* for a list of the environment variables you must set before using the `ldapbind` command.

To perform an SSL validation of the Oracle Virtual Directory instance on OVDHOST1, see the instructions in Section 4.6.1.1, "SSL Validation for Oracle Virtual Directory."

4.6.1.1 SSL Validation for Oracle Virtual Directory

Oracle Virtual Directory is configured to use the SSL Server Authentication Only Mode by default. When using command line tools like `ldapbind` to validate a connection using connection secured by SSL Server Authentication mode, the server certificate must be stored in an Oracle Wallet. Follow the steps below to perform this task:

1. Create an Oracle Wallet by executing the following command:

```
ORACLE_HOME/bin/orapki wallet create -wallet DIRECTORY_FOR_SSL_WALLET -pwd
WALLET_PASSWORD
```

2. Export the Oracle Virtual Directory server certificate by executing the following command:

```
ORACLE_HOME/jdk/jre/bin/keytool -exportcert -keystore OVD_KEYSTORE_FILE
-storepass PASSWORD -alias OVD_SERVER_CERT_ALIAS -rfc -file OVD_SERVER_CERT_
FILE
```

3. Add the Oracle Virtual Directory server certificate to the Oracle Wallet by executing the following command:

```
ORACLE_HOME/bin/orapki wallet add -wallet DIRECTORY_FOR_SSL_WALLET
-trusted_cert -cert OVD_SERVER_CERT_FILE -pwd WALLET_PASSWORD
```

4. Run the command below to verify that the Oracle Virtual Directory instance is listening on the SSL LDAP port. Use the wallet from Step 3:

```
ORACLE_HOME/bin/ldapbind -D "cn=orcladmin" -q -U 2 -h HOST -p SSL_PORT -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q
```

Note: If you are using default settings after installing 11*g* Release 1 (11.1.1), you can use the following values for the variables described in this section:

- For *OVD_KEYSTORE_FILE*, use:

  ```
  ORACLE_INSTANCE/config/OVD/ovd1/keystores/keys.jks
  ```

- For *OVD_SERVER_CERT_ALIAS*, use `serverselfsigned`
- For *PASSWORD* used for the `-storepass` option, use the orcladmin account password.
- *`OVD_SERVER_CERT_FILE`* refers to the file where the certificate is saved. The `keytool` utility creates this file under the location and filename specified by the *`OVD_SERVER_CERT_FILE`* parameter.

4.6.2 Installing an Additional Oracle Virtual Directory

Follow these steps to install the Release 11*g* Oracle Virtual Directory on OVDHOST2.

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "6501"
   netstat -an | grep "7501"
   ```

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

   On UNIX:

   Remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, or restart the computer.

4. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
5. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom ports:

   ```
   # The non-SSL port for Oracle Virtual Directory
   Oracle Virtual Directory port = 6501
   # The SSL port for Oracle Virtual Directory
   Oracle Virtual Directory (SSL) port = 7501
   ```

6. Start the Oracle Identity Management 11*g* Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.

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

   - **Specify the Inventory Directory**: `/u01/app/oraInventory`
   - **Operating System Group Name**: `oinstall`

     A dialog box appears with the following message:

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

     Log in as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

     ---

8. On the Welcome screen, click **Next**.
9. On the Select Installation Type screen, select **Install and Configure** and then click **Next**.
10. On the Prerequisite Checks screen, click **Next**.
11. On the Select Domain screen, select **Configure without a Domain**.

    Click **Next**.

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

    - **Oracle Home Location:**

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

    - **Oracle Instance Location:**

      `/u01/app/oracle/admin/ovd_inst2`

    - **Oracle Instance Name**:

```
ovd_inst2
```

Note: Ensure that the Oracle Home Location directory path for OVDHOST1 is the same as the Oracle Home Location directory path for OVDHOST2. For example, if the Oracle Home Location directory path for OVDHOST1 is:

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

then the Oracle Home Location directory path for OVDHOST2 must be:

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

Click **Next**.

13. On the Configure Components screen, select **Oracle Virtual Directory**, deselect all the other components, and click **Next**.
14. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.

    Click **Next**.
15. On the Specify Virtual Directory screen:

    In the Client Listeners section, enter:

    - LDAP v3 Name Space:

      ```
      dc=us,dc=mycompany,dc=com
      ```

    In the OVD Administrator section, enter:

    - Administrator User Name: `cn=orcladmin`
    - Password: `*******`
    - Confirm Password: `*******`

    Select **Configure the Administrative Server in secure mode**.

    Click **Next**.
16. 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**.
17. On the Installation Progress screen on UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window.

    Click **Next**.
18. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait for the configuration process to finish.
19. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
20. To validate the installation of the Oracle Virtual Directory instance on OVDHOST2, issue this command:

```
ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
```

Note: See the "Configuring Your Environment" section of *Oracle Fusion Middleware User Reference for Oracle Identity Management* for a list of the environment variables you must set before using the `ldapbind` command.

To perform an SSL validation of the Oracle Virtual Directory instance on OVDHOST2, see the instructions in Section 4.6.1.1, "SSL Validation for Oracle Virtual Directory." Also, the wallet on each node should contain certificates from both OVDHOST1 and OVDHOST2. Step 3 in Section 4.6.1.1, "SSL Validation for Oracle Virtual Directory" describes how to add a certificate to a wallet.

4.6.3 Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain

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

To register the Oracle Virtual Directory instances installed on OVDHOST1 and OVDHOST2, follow these steps:

1. Set the ORACLE_HOME variable. For example, on OVDHOST1 and OVDHOST2, issue this command:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/fmw/idm
   ```

2. Set the ORACLE_INSTANCE variable. For example:

   On OVDHOST1, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd_inst1
   ```

   On OVDHOST2, issue this command:

   ```
   export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd_inst2
   ```

3. Execute the opmnctl registerinstance command on both OVDHOST1 and OVDHOST2:

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

   For example, on OVDHOST1 and OVDHOST2:

   ```
   ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost idmhost1.mycompany.com
   -adminPort 7001 -adminUsername weblogic

   Command requires login to weblogic admin server (idmhost1.mycompany.com)
    Username: weblogic
    Password: *******
   ```

Note: For additional details on registering Oracle Internet Directory components with a WebLogic Server domain, see the "Registering a System Component Domain Using OPMNCTL" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

4.6.4 Configuring Oracle Virtual Directory Communication with LDAP

Oracle Virtual Directory uses adapters to connect to its underlying data repositories so it can virtualize data and route data to and from the repositories. Oracle Virtual Directory uses an LDAP Adapter to connect to an underlying LDAP repository.

Note: Do not configure Oracle Virtual Directory communication with LDAP until after Oracle Directory Services Manager is installed in Section 5.1, "Extending the Oracle WebLogic Domain with DIP and ODSM."

The LDAP Adapter enables Oracle Virtual Directory to present data as a sub tree of the virtual directory by proving real-time directory structure and schema translations. One LDAP Adapter is required for each distinct LDAP source you want to connect to. For example, if you have two LDAP repositories that are replicas of each other, you would deploy one LDAP Adapter and configure it to list the hostnames and ports of the replicas.

Note: If you plan on using a LDAP repository other than Oracle Internet Directory in your environment, you are required to configure a LDAP Adapter to connect to that repository. For more information on creating and configuring an LDAP Adapter, refer to the "Creating and Configuring Oracle Virtual Directory Adapters" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

4.7 Validating the Directory Tier Components

To validate the directory tier components, ensure that you can connect to each Oracle Internet Directory instance and the load balancing router using these commands:

Note: See the "Configuring Your Environment" section of *Oracle Fusion Middleware User Reference for Oracle Identity Management* for a list of the environment variables you must set before using the `ldapbind` command.

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

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

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

Note: The -q option above prompts the user for a password. LDAP tools have been modified to disable the options -w *password* and -P *password* when the environment variable LDAP_PASSWORD_PROMPTONLY is set to TRUE or 1. Use this feature whenever possible.

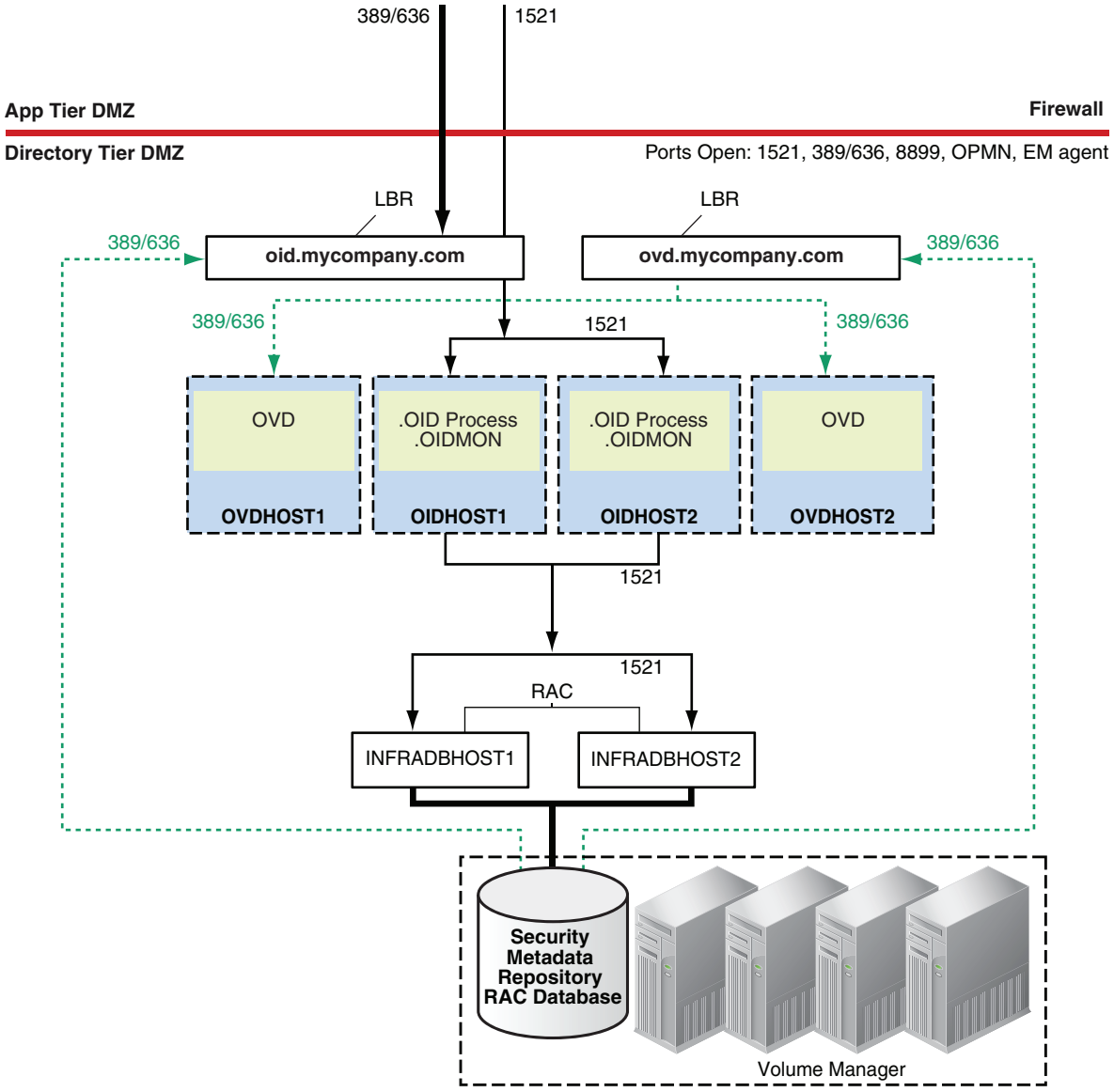
Follow the steps in Section 4.6.1.1, "SSL Validation for Oracle Virtual Directory" before running the `ldapbind` command with the SSL port. Test each Oracle Virtual Directory instance and the load balancing router using these commands:

```
ldapbind -h ovdhost1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q

ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q

ldapbind -h ovd.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h ovd.mycompany.com -p 636 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q
```

Note: The wallets on OVDHOST1 and OVDHOST2 must contain the client certificates from both OVDHOST1 and OVDHOST2, when connecting to the Oracle Virtual Directory instances using the load balancing router host and SSL port.

The directory tier configuration is now as shown in Figure 4–1.

Figure 4–1 Directory Tier Configuration



4.8 Backing Up the Directory Tier Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restore in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

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

To back up the installation to this point, follow these steps:

1. Back up the directory tier:
   a. Shut down the instance using `opmnctl` located under the *ORACLE_INSTANCE*`/bin` directory:

      ```
      ORACLE_INSTANCE/bin/opmnctl stopall
      ```

   b. Create a backup of the Middleware Home on the directory tier as the `root` user:

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

   c. Create a backup of the Instance Home on the directory tier as the `root` user:

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

   d. Start up the instance using `opmnctl` located under the *ORACLE_INSTANCE*`/bin` directory:

      ```
      ORACLE_INSTANCE/bin/opmnctl startall
      ```

2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. An operating system tool such as `tar` can be used for cold backups.
3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the *MW_HOME*`/user_projects/domains/`*domainName* directory:

   ```
   IDMHOST1> tar cvf edgdomainback.tar MW_HOME/user_projects/domains/domainName
   ```

   Note: Create backups on all machines in the directory tier by following the steps shown above.

For more information about backing up the directory tier configuration, see Section 10.4, "Performing Backups and Recoveries."

5

Installing and Configuring Oracle DIP and ODSM

This chapter describes how to install and configure Oracle Directory Integration Platform (DIP) and Oracle Directory Services Manager (ODSM).

This chapter includes the following topics:

5.1 Extending the Oracle WebLogic Domain with DIP and ODSM

The application tier consists of multiple computers hosting the Oracle Directory Integration Platform, Oracle Directory Services Manager, and Oracle Access Manager instances. In the complete configuration, requests are balanced among the instances on the application tier computers to create a performant and fault tolerant application environment.

> **Note:** Oracle Directory Integration Platform uses Quartz to maintain its jobs and schedules in the database. For the Quartz jobs to be run on different Oracle Directory Integration Platform nodes in a cluster, it is recommended that the system clocks on the cluster nodes be synchronized.

Follow these steps to install and configure Oracle Directory Integration Platform and Oracle Directory Services Manager on IDMHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Ensure that port 7006 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "7006"
   ```

If the port is in use (if the command returns output identifying the port), you must free it.

On UNIX:

Remove the entries for port 7006 in the `/etc/services` file and restart the services, or restart the computer.

3. Copy the `staticports.ini` file from the Disk1/stage/Response directory to a temporary directory.
4. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

```
# The port for ODSM Server port
ODS Server Port No = 7006
```

5. Start the Oracle Identity Management 11*g* Configuration Assistant by running the `config.sh` script located under the *`ORACLE_HOME`*`/bin` directory on IDMHOST1. For example:

```
/u01/app/oracle/product/fmw/idm/bin/config.sh
```

6. On the Welcome screen, click **Next**.
7. On the Select Domain screen, select **Extend Existing Domain** and enter the domain details:
   - **Host Name**: `idmhost1.mycompany.com`
   - **Port**: 7001
   - **User Name:** `weblogic`
   - **User Password:** `<enter user password>`

   Click **Next**.
8. On the Specify Installation Location screen, specify the following values (the values for the Oracle Middleware Home Location and the Oracle Home Directory fields are prefilled. The values default to the Middleware Home and Oracle Home previously installed on IDMHOST1 in Section 3.2, "Configuring the WebLogic Server Domain on IDMHOST1":
   - **Oracle Middleware Home Location:**

     `/u01/app/oracle/product/fmw`
   - **Oracle Home Directory**: idm
   - **WebLogic Server Directory**:

     `/u01/app/oracle/product/fmw/wlserver_10.3`
   - **Oracle Instance Location:**

     `/u01/app/oracle/admin/idm_inst1`
   - **Oracle Instance Name**:

     `idm_inst1`

   Click **Next**.
9. On the Specify Email for Security Updates screen, specify these values:

- **Email Address**: Provide the email address for your My Oracle Support account.
- **Oracle Support Password**: Provide the password for your My Oracle Support account.
- Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

10. On the Configure Components screen, select **Oracle Directory Integration Platform, Management Components - Oracle Directory Services Manager** and deselect all the other components.

    Select the **Clustered** check box.

    Click **Next**.

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

    Click **Next**.

12. On the Specify OID Details screen, specify the following:
    - **Hostname:** `oid.mycompany.com`
    - **Port**: 389
    - **Username:** `cn=orcladmin`
    - **Password:** `******`

    Click **Next**.

13. On the Specify Schema Database screen, specify the following values:
    - Connect String:

      ```
      infradbhost1-vip.mycompany.com:1521:idmdb1^infradbhost2-vip.mycompany.com:1
      521:idmdb2@idmedg.mycompany.com
      ```

      Note: The RAC database connect string information needs to be provided in the format *host1*:*port1*:*instance1*^*host2*:*port2*:*instance2*@*servicename*.

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

      It is required that the information provided above is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each RAC instance, and the service name provided must be configured for all the specified RAC instances.

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

    - User Name: `ODSSM`
    - Password: `******`

    Click **Next**.

14. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Configure**.
15. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.
16. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

5.2 Expanding the DIP and ODSM Cluster

The following sections include the steps for extending the WebLogic Server Domain on IDMHOST2:

- Section 5.2.1, "Install and Configure DIP and ODSM on IDMHOST2"
- Section 5.2.2, "Post-Installation Steps"

5.2.1 Install and Configure DIP and ODSM on IDMHOST2

Follow these steps to install and configure Oracle Directory Integration Platform and Oracle Directory Service Manager on IDMHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Ensure that port number 7006 is not in use by any service on the computer by issuing this command for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "7006"
   ```

   If the port is in use (if the command returns output identifying the port), you must free it.

   On UNIX:

   Remove the entries for port 7006 in the `/etc/services` file if the port is in use by a service and restart the services, or restart the computer.
3. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
4. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

   ```
   #The port for ODSM Server port
   ODS Server Port No: 7006
   ```

5. Start the Oracle Identity Management 11g Installer as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

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

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

Operating System Group Name: `oinstall`

A dialog box appears with the following message:

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

Login as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

---

7. On the Welcome screen, click **Next**.
8. On the Select Installation Type screen, select **Install and Configure** and then click **Next**.
9. On the Prerequisite Checks screen, the installer completes the prerequisite checks. If any fail, please fix them and restart your Installation.

   Click **Next**.
10. On the Select Domain screen, select the **Expand Cluster** option and specify these values:
    - **Hostname:** `idmhost1.mycompany.com`
    - **Port**: `7001`
    - **UserName**: `weblogic`
    - **User Password**: `<Enter the password for the webLogic user>`

    Click **Next**.
11. On the Specify Installation Location screen, specify these values:
    - **Oracle Middleware Home Location:**

      `/u01/app/oracle/product/fmw`
    - **Oracle Home Directory**: idm
    - **WebLogic Server Directory**:

      `/u01/app/oracle/product/fmw/wlserver_10.3`
    - **Oracle Instance Location**:

```
/u01/app/oracle/admin/idm_inst2
```

- **Oracle Instance Name**: idm_inst2

Click **Next**.

12. On the Email for Security Updates screen, specify these values:
    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.
13. On the Configure Components screen, de-select all the products except **Oracle DIP and Management Components** and then click **Next**.
14. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.

    Click **Next**.
15. 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**.
16. On the Installation Progress screen on UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window, log in as root, and run the script, following the prompts in the window.

    Click **Next**.
17. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.
18. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

5.2.2 Post-Installation Steps

In the previous section, the installer created a second Managed Server, wls_ods2 on IDMHOST2. However, the Oracle Directory Integration Platform application is not deployed on IDMHOST2 and the newly created Managed Server is not automatically started. Also, the WebLogic Administration Console shows the state of the wls_od2 Managed Server on IDMHOST2 as UNKNOWN.

Follow the post-installation steps in this section to complete the installation and configuration of the Oracle Directory Integration Platform and Oracle Directory Services Manager applications on IDMHOST2.

5.2.2.1 Copy the DIP Application from IDMHOST1 to IDMHOST2

Follow these steps to copy the Oracle Directory Integration Platform application from IDMHOST1 to IDMHOST2:

1. On IDMHOST2, create the following directory structure:

   MW_HOME`/user_projects/domains/IDMDomain/servers/wls_ods2/stage/DIP/11.1.1.1.0`

   For example:

```
mkdir -p MW_HOME/user_projects/domains/IDMDomain/servers/wls_
ods2/stage/DIP/11.1.1.1.0/
```

2. Copy the DIP directory from IDMHOST1 to IDMHOST2.

   Copy the following directory on IDMHOST1:

   ```
   MW_HOME/user_projects/domains/IDMDomain/servers/wls_
   ods1/stage/DIP/11.1.1.1.0/DIP
   ```

   to the following location on IDMHOST2:

   ```
   MW_HOME/user_projects/domains/IDMDomain/servers/wls_ods2/stage/DIP/11.1.1.1.0/
   ```

   For example, from IDMHOST1, execute this command:

   ```
   scp -rp MW_HOME/user_projects/domains/IDMDomain/servers/wls_ods1/stage/
   DIP/11.1.1.1.0/DIP user@IDMHOST2://MW_HOME/user_projects/domains/IDMDomain/
   servers/wls_ods2/stage/DIP/11.1.1.1.0
   ```

5.2.2.2 Set the Listen Address for the Managed Servers

Set the listen address for the `WLS_ODS1` and `WLS_ODS2` Managed Servers to the host name of their respective nodes using the Oracle WebLogic Administration Server:

1. Using a web browser, bring up the Oracle WebLogic Administration Server console and log in using the `weblogic` user credentials.
2. In the left pane of the WebLogic Administration Server Console, click **Lock & Edit** to edit the server configuration.
3. In the left pane of the WebLogic Server Administration Console, expand **Environment** and select **Servers**.
4. On the Summary of Servers page, click on the link for the `wls_ods1` Managed Server.
5. On the Settings page for the `wls_ods1` Managed Server, update the Listen Address to `idmhost1.mycompany.com`. This is the host name of the server where `wls_ods1` is running.
6. Click **Save** to save the configuration.
7. Repeat steps 2 to 6 to update the Listen Address for the `wls_ods2` Managed Server to `idmhost2.mycompany.com`. This is host name of the server where `wls_ods2` is running.
8. Click **Activate Changes** to update the server configuration.

5.2.2.3 Start the wls_ods2 Managed Server on IDMHOST2

Follow these steps to start the newly created `wls_ods2` Managed Server in a cluster on IDMHOST2:

1. In the left pane of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Clusters**.
2. Select the cluster (`cluster_ods`) containing the Managed Server (`wls_ods2`) you want to start.
3. Select **Control**.
4. Under **Managed Server Instances in this Cluster**, select the check box next to the Managed Server (`wls_ods2`) you want to start and click **Start**.

5. On the Server Life Cycle Assistant page, click **Yes** to confirm.

Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

5.3 Validating the Application Tier Configuration

This section includes steps for validating Oracle Directory Services Manager and Oracle Directory Integration Platform.

5.3.1 Validating Oracle Directory Services Manager

Follow these steps to validate the Oracle Directory Services Manager installation:

1. Bring up the Oracle Directory Services Manager (ODSM) Administration Console in a web browser. The URL to access the ODSM Administration Console is:

   `http://`*`hostname`*`.mycompany.com:`*`port`*`/odsm/faces.odsm.jspx`

   For example, on IDMHOST1, enter this URL:

   `http://idmhost1.mycompany.com:7006/odsm/faces/odsm.jspx`

   And on IDMHOST2, enter this URL:

   `http://idmhost2.mycompany.com:7006/odsm/faces/odsm.jspx`

2. Validate that Oracle Directory Services Manager can create connections to Oracle Internet Directory and Oracle Virtual Directory. Follow these steps to create connections to Oracle Internet Directory and Oracle Virtual Directory:

   To create connections to Oracle Internet Directory, follow these steps:

   a. Launch Oracle Directory Services Manager from IDMHOST1:

      `http://idmhost1.mycompany.com:7006/odsm/faces/odsm.jspx`

   b. Create a connection to the Oracle Internet Directory virtual host by providing the information shown below in the ODSM Console:

      ```
      Host: oid.mycompany.com
      Port: 636
      Enable the SSL option
      User: cn=orcladmin
      Password: <ldap-password>
      ```

   To create connections to Oracle Virtual Directory, follow these steps. Create connections to each Oracle Virtual Directory node separately. Using the Oracle Virtual Directory load balancer virtual host from the ODSM Console is not supported:

   a. Launch Oracle Directory Services Manager from IDMHOST1:

      `http://idmhost1.mycompany.com:7006/odsm/faces/odsm.jspx`

   b. Create a direct connection to Oracle Virtual Directory on OVDHOST1 providing the information shown below in the ODSM Console:

      ```
      Host: ovdhost1.mycompany.com
      Port: 8899  (The Oracle Virtual Directory proxy port)
      Enable the SSL option
      User: cn=orcladmin
      ```

```
Password: <ldap-password>
```

5.3.2 Validating Oracle Directory Integration Platform

Validate the Oracle Directory Integration Platform installation by using the WLST `dipStatus` command. To run this command, follow these steps:

1. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries. For example:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/fmw/idm
   ```

2. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server. For example:

   ```
   export WLS_HOME=/u01/app/oracle/product/fmw/wlserver_10.3
   ```

3. Run the *ORACLE_HOME*`/bin/dipStatus -h` *hostName* `-p` *port* `-D` *wlsuser* command.

   For example, on IDMHOST1, the command and output look like this:

   ```
   ORACLE_HOME/bin/dipStatus -h idmhost1.mycompany.com -p 7006 -D weblogic
   [Weblogic user password]
   Connection parameters initialized.
   Connecting at idmhost1.mycompany.com:7006, with userid "weblogic"..
   Connected successfully.

   ODIP Application is active at this host and port.
   ```

   For example, on IDMHOST2, the command and output look like this:

   ```
   ORACLE_HOME/bin/dipStatus -h idmhost2.mycompany.com -p 7006 -D weblogic
   [Weblogic user password]
   Connection parameters initialized.
   Connecting at idmhost2.mycompany.com:7006, with userid "weblogic"..
   Connected successfully.

   ODIP Application is active at this host and port.
   ```

5.4 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restore in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

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

To back up the installation to this point, follow these steps:

1. Back up the application tier:

a. Shut down the instance using `opmnctl` located under the *ORACLE_INSTANCE*`/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

b. Create a backup of the Middleware Home on the application tier as the `root` user:

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

c. Create a backup of the Instance Home on the application tier as the `root` user:

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

d. Start up the instance using `opmnctl` located under the *ORACLE_INSTANCE*`/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. An operating system tool such as `tar` can be used for cold backups.
3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the *MW_HOME*`/user_projects/domains/`*domainName* directory:

```
IDMHOST1> tar cvf edgdomainback.tar MW_HOME/user_projects/domains/domainName
```

Note: Create backups on all machines in the application tier by following the steps shown above.

For information about backing up the application tier configuration, see Section 10.4, "Performing Backups and Recoveries."

6

Installing and Configuring the Web Tier

This chapter describes how to install and configure the components on the web tier. The web tier runs the Oracle HTTP Server component and a load balancer.

This chapter includes the following topics:

6.1 Prerequisites

- Ensure that the system, patch, kernel, and other requirements are met as specified in the installation guide.
- Ensure that port 7777 is not used by any service on the nodes. You can check by running these commands. If the ports are in use, you must free the ports.

  On UNIX: `netstat -an | grep "7777"`

6.2 Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2

Follow these steps to install Oracle HTTP Server on WEBHOST1 and WEBHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Web Tier* in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. Oracle HTTP Server is installed on port 7777 by default. Ensure that ports 7777, 8889, and 4443 are not in use by any service on WEBHOST1 or WEBHOST2 by issuing these commands for the operating system you are using:

   On UNIX:

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

```
netstat -an | grep "8889"
netstat -an | grep "4443"
```

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

On UNIX:

Remove the entries for ports 7777, 8889, and 4443 in the `/etc/services` file if the ports are in use by a service and restart the services, or restart the computer.

3. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
4. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

```
#The http_main port for ohs component
OHS Port = 7777

#This port indicates the OHS proxy port
OHS Proxy Port = 8889

#This port indicates the OHS SSL port
OHS SSL Port = 4443
```

5. Start the Oracle Universal Installer for Oracle Fusion Middleware 11*g* Web Tier Utilities CD installation as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.

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

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

   Operating System Group Name: `oinstall`

   A dialog box appears with the following message:

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

   Login as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

7. On the Welcome screen, click **Next**.
8. On the Select Installation Type screen, select **Install and Configure**, and click **Next**.
9. On the Prerequisite Checks screen, ensure that all the prerequisites are met, then click **Next**.
10. On the Specify Installation Location screen:

    On both WEBHOST1 and WEBHOST2, set the **Location** to:

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

    Click **Next**.
11. On the Configure Components screen:
    - Select **Oracle HTTP Server**.
    - Select **Associate Selected Components with WebLogic Domain**.

    Click **Next**.
12. On the Specify WebLogic Domain screen:

    Enter the following values:
    - **Domain Host Name**: `IDMHOST1`
    - **Domain Port No**: `7001`
    - **User Name**: `weblogic`
    - **Password**: `******`

    Click **Next**.
13. On the Specify Component Details screen:
    - Enter the following values for WEBHOST1:
      - **Instance Home Location**: `/u01/app/oracle/admin/ohs_inst1`
      - **Instance Name**: `ohs_inst1`
      - **OHS Component Name**: `ohs1`
    - Enter the following values for WEBHOST2:
      - **Instance Home Location**: `/u01/app/oracle/admin/ohs_inst2`
      - **Instance Name**: `ohs_inst2`
      - **OHS Component Name**: `ohs2`

    Click **Next**.

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

    Click **Next**.

15. On the Installation Summary screen, ensure that the selections are correct, and click **Install**.

16. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Configuration Completed screen appears.

17. On the Configuration Completed screen, click **Finish** to exit.

6.3 Validating the Installations of Oracle HTTP Server

In a web browser, go to the following URLs to validate that the installations of Oracle HTTP Server were successful:

```
http://webhost1.mycompany.com:7777
http://webhost2.mycompany.com:7777
```

6.4 Configuring Oracle HTTP Server with the Load Balancer

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server (`WEBHOST1`, `WEBHOST2`).

You do not need to enable sticky session (insert cookie) on the load balancer when Oracle HTTP Server is front-ending Oracle WebLogic Server. You need sticky session if you are going directly from the load balancer to Oracle WebLogic Server, which is not the case in the topology described in this guide.

Also, you should set Monitors for HTTP.

6.5 Configuring Oracle HTTP Server for Virtual Hosts

The Oracle HTTP Server instances on WEBHOST1 and WEBHOST2 should be configured to use the virtual hosts set up in the load balancer.

To configure the Oracle HTTP Server instances to use the load balancer router virtual hosts, define the Virtual Host directives in the <VirtualHost> section of the httpd.conf file on each of the Oracle HTTP Server instances.

The httpd.conf file is located under the following directory on WEBHOST1 and WEBHOST2.

ORACLE_INSTANCE/config/OHS/<componentName>

Open the httpd.conf file in a text editor and add the following directives on WEBHOST1 and WEBHOST2:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName https://sso.mycompany.com:443
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>
```

```
NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>
```

6.6 Configuring mod_wl_ohs for Oracle WebLogic Server Clusters

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle WebLogic Server clusters, add the directives shown below to the `mod_wl_ohs.conf` file on both WEBHOST1 and WEBHOST2.

The `mod_wl_ohs.conf` file is located under the following directory on WEBHOST1 and WEBHOST2:

ORACLE_INSTANCE/config/OHS/*componentName*

1. In a text editor, add the following lines to the mod_wl_ohs.conf file on WEBHOST1 and WEBHOST2:

```
LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

<IfModule mod_weblogic.c>
WebLogicHost idmhost1.mycompany.com
WebLogicPort 7001
</IfModule>

# Admin Server and EM
<Location /console>
SetHandler weblogic-handler
WebLogicHost idmhost1.mycompany.com
WeblogicPort 7001
</Location>

<Location /consolehelp>
SetHandler weblogic-handler
WebLogicHost idmhost1.mycompany.com
WeblogicPort 7001
</Location>

<Location /em>
SetHandler weblogic-handler
WebLogicHost idmhost1.mycompany.com
WeblogicPort 7001
</Location>

#Oracle Directory Services Manager
<Location /odsm>
SetHandler weblogic-handler
WebLogicCluster idmhost1.mycompany.com:7006,idmhost2.mycompany.com:7006
</Location>
```

2. Restart Oracle HTTP Server:

```
ORACLE_INSTANCE/bin/opmnctl restartproc ias-component=ohs1
```

3. Verify that you can access all these URLs:

Oracle Directory Services Manager Console:

```
http://admin.mycompany.com:7777/odsm
```

Oracle WebLogic Server Administration Console:

```
http://admin.mycompany.com:7777/console
```

Oracle Enterprise Manager Fusion Middleware Control:

```
http://admin.mycompany.com:7777/em
```

The servers specified in the `WebLogicCluster` parameter are only important at startup time for the plug-in. The list needs to provide at least one running cluster member for the plug-in to discover other members of the cluster. Note that the listed cluster member must be running when the Oracle HTTP Server is started up. Oracle WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Some example scenarios:

- Example 1: If you have a two-node cluster and then add a third member, you do not need to update the configuration to add the third member. The third member will be discovered on the fly at runtime.
- Example 2: You have a three-node cluster but only two nodes are listed in the configuration. However, if both listed nodes are down when you start up Oracle HTTP Server, then the plug-in would fail to route to the cluster. You need to ensure that at least one of the listed nodes is running when you start up Oracle HTTP Server.

  If you list all members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started.

For more information on configuring the WebLogic Server plug-in, see *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server*.

6.7 Setting the Frontend URL for the Administration Console

In the Identity Management topology described in this manual, since the Oracle WebLogic Server Administration Console is frontended by an Oracle HTTP Server and a load balancing router, perform the following steps:

1. Log into the Oracle WebLogic Server Administration Server Console.
2. In the Change Center, click **Lock and Edit** to enable configuration changes.
3. In the Environment section of the Home page, click **Servers**.
4. On the Summary of Servers page, click the **AdminServer** link.
5. On the Admin Server Settings page, click the **Protocols** tab.
6. Under the **Protocols** tab, click on the **HTTP** tab.
7. On the HTTP page, set the following values:
   - **Frontend Host**: Specify the load balancing router address. For example: `admin.mycompany.com`
   - **Frontend Port**: Specify the load balancing router port: For example: `7777`
8. Click **Save** to save the configuration.

9. Click **Activate Changes** to update the configuration.

6.8 Validating the Web Tier Configuration

To validate that you have configured the load balancer virtual hosts correctly, check that you can access these URLs:

Oracle Directory Services Manager Console:

```
http://admin.mycompany.com:7777/odsm
```

Oracle WebLogic Server Administration Console:

```
http://admin.mycompany.com:7777/console
```

Oracle Enterprise Manager Fusion Middleware Control:

```
http://admin.mycompany.com:7777/em
```

Single Sign-On URL:

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

Note: The single sign-on (SSO) URL will return the default Oracle HTTP Server page, since SSO has not yet been configured.

6.9 Backing up the Web Tier Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restore in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier:
   a. Shut down the instance using `opmnctl` located under the *`ORACLE_INSTANCE`*`/bin` directory:

      ```
      ORACLE_INSTANCE/bin/opmnctl stopall
      ```

   b. Create a backup of the Middleware Home on the web tier as the `root` user:

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

   c. Create a backup of the Instance Home on the web tier as the `root` user:

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

   d. Start up the instance using `opmnctl` located under the *`ORACLE_INSTANCE`*`/bin` directory:

      ```
      ORACLE_INSTANCE/bin/opmnctl startall
      ```

2. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the *MW_HOME*`/user_projects/domains/`*domainName* directory:

```
IDMHOST1> tar cvf edgdomainback.tar MW_HOME/user_projects/domains/domainName
```

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

For information about backing up the web tier configuration, see Section 10.4, "Performing Backups and Recoveries"?

7

Installing and Configuring Oracle Access Manager

This chapter describes how to install and configure Oracle Access Manager 10.1.4.3 for use in the Oracle Identity Management enterprise deployment.

This chapter includes the following topics:

7.1 Introduction to Installing Oracle Access Manager

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

Oracle Access Manager consists of various components including Access Server, Identity Server, WebPass, Policy Manager, WebGates, AccessGates, and Access SDK. The Access Server and Identity Server are the server components necessary to serve user requests for access to enterprise resources. Policy Manager and WebPass are the administrative consoles to the Access Server and Identity Server respectively. WebGates are web server agents that act as the actual enforcement points for Oracle Access Manager while AccessGates are the application server agents. Finally, the Access SDK is a toolkit provided for users to create their own WebGate or AccessGate should the out-of-the-box solutions be insufficient. Follow the instructions in this chapter and Chapter 8, "Configuring Single Sign-On for Administration Consoles" to install and configure the Oracle Access Manager components necessary for your enterprise deployment.

For more information about Oracle Access Manager 10.1.4.3 and its various components, refer to the "Road Map to Manuals" section in the *Oracle Access Manager*

Introduction manual, which includes a description of each manual in the Oracle Access Manager 10.1.4.3 documentation set.

7.1.1 Using 10*g* Oracle Single Sign-On and Delegated Administration Services

This manual recommends Oracle Access Manager as the single sign-on solution. However, for customers who have deployed 10*g* Oracle Single Sign-on and would like to continue to use that as a solution, they can do so. In cases where customers have deployed Oracle E-Business Suite, have deployed or will be deploying Portal, Forms, Reports or Discoverer, Oracle Single Sign-On and Oracle Delegated Administration Service are mandatory components.

Oracle Single Sign-On and Oracle Delegated Administration Service are not part of the 11*g* release. Customers must download the 10.1.4.* versions of these products, which are compatible with 11*g* Oracle Internet Directory and Oracle Directory Integration Platform, to form what was known in 10*g* as the Application Server Infrastructure. For deployment instructions on these 10*g* products, please read Chapter 4 "Installing and Configuring JAZN-SSO/DAS" in the *Oracle Application Server Enterprise Deployment Guide* (B28184-02) for Oracle Identity Management release 10.1.4.0.1. This manual is available on Oracle Technology Network at:

`http://download.oracle.com/docs/cd/B28196_01/core.1014/b28184/toc.htm`

7.1.2 Using Different LDAP Directory Stores

This enterprise deployment described in this manual (Figure 1–1) shows Oracle Access Manager using Oracle Internet Directory as the only LDAP repository. Oracle Access Manager uses a single LDAP for policy and configuration data. It is possible to configure another LDAP as the identity store where users, organizations and groups reside. For example, an Oracle Access Manager instance may use Oracle Internet Directory as its policy and configuration store and point to an instance of Microsoft Active Directory for users and groups.

7.1.2.1 Using Oracle Virtual Directory as the Identity Store

In addition, the identity stores can potentially be front-ended by Oracle Virtual Directory to virtualize the data sources.

To learn more about the different types of directory configuration for Oracle Access Manager, please consult the 10*g* Oracle Access Manager documentation at Oracle Technology Network. Customers considering these variations should adjust their directory tier and Oracle Access Manager deployment accordingly.

7.2 Prerequisites

These are the basic prerequisites for installing Oracle Access Manager components:

- On Linux systems, you are prompted at component install time to provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with the GCC 3.3.2 runtime libraries. These files are available from Oracle Technology Network at:

  `http://www.oracle.com/technology/software/products/ias/htdocs/101401.html`

- Copy these libraries to a location accessible from the host where Oracle Access Manager is being installed. For example, use the home directory of the user installing Oracle Access Manager. In this case it is `/home/oracle`
- There is a known bug with the Oracle Access Manager installer that sometimes manifests as a hang at install time on Linux. This is a third-party issue caused by InstallShield.

  To work around this issue, follow these steps:

  1. Copy and paste the following in the shell where you start the installer:

     ```
     cd /tmp
     mkdir bin.$$
     cd bin.$$
     cat > mount <<EOF
     #! /bin/sh
     exec /bin/true
     EOF
     chmod 755 mount
     export PATH=`pwd`:$PATH
     ```

  2. Run the installation.
  3. When the installer is finished running, clean the temporary directory using this command:

     ```
     rm -r /tmp/bin.$$
     ```

- For a complete list of prerequisites, refer to the *Oracle Access Manager Installation Guide*.

7.3 Identity System Installation and Configuration

This section provides steps to install and configure the Oracle Access Manager Identity System. The Identity System components include Identity Server and WebPass.

7.3.1 Installing Identity Servers on OAMHOST1 and OAMHOST2

The following sections describe how to install Oracle Access Manager Identity Server on OAMHOST1 and OAMHOST2.

7.3.1.1 Installing the First Identity Server on OAMHOST1

Follow these steps to install Oracle Access Manager Identity Server on OAMHOST1:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Identity Server" chapter of the *Oracle Access Manager Installation Guide*.
2. Locate the Identity Server Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the Installers GUI console:

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_Identity_Server -gui
   ```

3. On the Welcome to the InstallShield Wizard for Oracle Access Manager Identity Server screen, click **Next**.
4. Enter the username and group that the Identity Server will use. Specify `oracle/oinstall`.

Click **Next**.

5. Specify the installation directory for Oracle Access Manager Identity Server. Specify the following value:

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

   Note: The base location for the Oracle Access Manager installation is `/u01/app/oracle/product/fmw/oam`. Oracle Access Manager components are installed in subdirectories automatically created by the installer under this location.

   The Identity Server is installed in the `identity` subdirectory created by the installer under the base location.

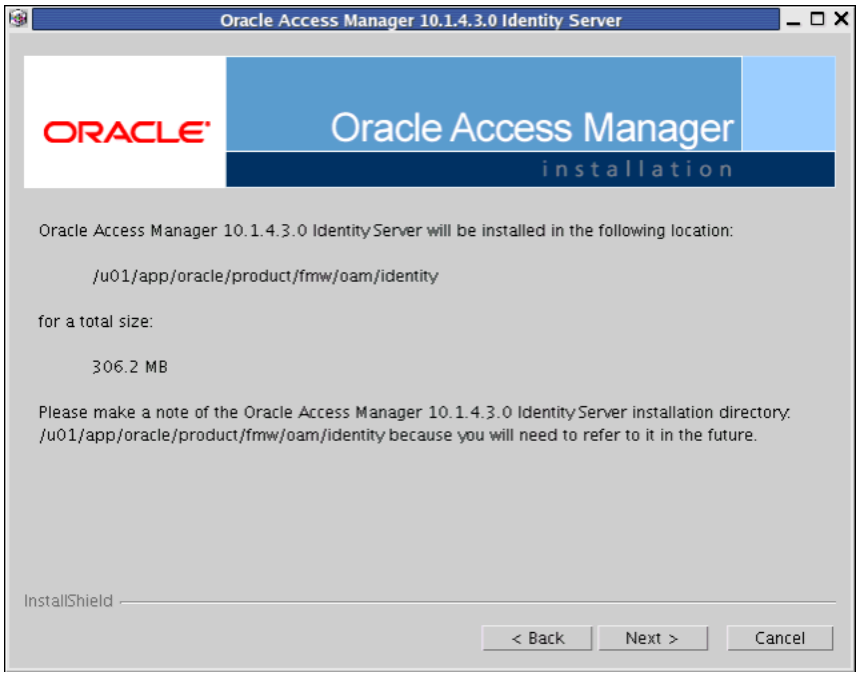
   The ORACLE_HOME location for the Oracle Access Manager Identity Server installation is:

   `/u01/app/oracle/product/fmw/oam/identity`

   Click **Next**.

6. Oracle Identity Manager will be installed in the following location (the `identity` directory is created by the installer automatically):

   `/u01/app/oracle/product/fmw/oam/identity`



7. Specify the location of the GCC runtime libraries, for example, `/home/oracle/oam_lib`.

   Click **Next**.

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

9. On the first Identity Server Configuration screen, specify the transport security mode between the WebPass/Identity client and the Identity Server. The choices are:

   - **Open Mode**: No encryption.
   - **Simple Mode**: Encryption through SSL and a Public Key Certificate provided by Oracle.
   - **Cert Mode**: Encryption through SSL and a Public Key Certificate provided by an external CA.

   Choose **Open Mode**.

   Click **Next**.

10. On the next Identity Server Configuration screen, specify the Identity Server ID, host name and port number for the Identity Server connection:

    - Enter a unique name for the Identity Server ID. For example: `IdentityServer_OAMHOST1`
    - Enter the hostname where the Identity Server will be installed. Make sure that the hostname can be resolved. For example: `oamhost1.mycompany.com`
    - Enter the port number on which this Identity Server communicates with its clients. For example, the default port number is 6022.

    Click **Next**.

11. On the next Identity Server Configuration screen, you are prompted whether this is the first Identity Server installation in the network for this LDAP directory server.

    Select **Yes**.

    Click **Next**.

12. On the next Identity Server Configuration screen, select the appropriate options if you want to set up SSL between the Identity Server and the Directory Server.

    - Directory Server hosting user data is in SSL
    - Directory Server hosting Oracle data is in SSL

    The enterprise deployment described in this manual does not use SSL for communication between components behind the firewall.

    Do not select anything.

    Click **Next**.

13. On the first Configure Directory Server hosting user data screen, specify the details for the LDAP enabled User Directory Store.

    The Identity Server connects to an LDAP enabled directory server to store your User Data. Choose the appropriate directory server from the drop down list:

    - If you are planning on using Oracle Virtual Directory as the user store; select **Data Anywhere** from the drop down list.
    - If you are planning on using Oracle Internet Directory for the user store, select **Oracle Internet Directory** from the drop down list.

    Make the appropriate choice based on the needs in your environment and click **Next**.

14. On the next Configure Directory Server hosting user data screen, specify if the User and Oracle Data will be stored in different directory servers. Make the appropriate choice based on the requirements in your environment.

    Select the **Oracle data will be in the user data directory** option.

    The enterprise deployment in this manual has the Oracle and user data in the same directory.

    Click **Next**.

15. On the next Configure Directory Server hosting user data screen, specify if the OAM Installer should automatically update the User Store Directory Schema to include the Oracle Access manager schema

    Select **Yes** and click **Next**.

16. Specify your directory server configuration details:

    - **Host machine or IP in which the directory server resides**:

      `oid.mycompany.com` (if your user store is in Oracle Internet Directory)

      `ovd.mycompany.com` (if your user store is in Oracle Virtual Directory)

    - **Port Number**: `389` (non-SSL port)
    - **Root DN**: `cn=orcladmin` (This is the default, unless you change the person object class during Identity System set up.)
    - **Root Password**: The password for the user data directory server Root DN.

    Click **Next**.

17. The Updating Directory schema to Directory Server screen appears. The update process can take some time.

18. Review the Readme file.

    Click **Next** to display an installation summary.

19. The installation summary provides the details that you specified during this installation and instructs you to start the Identity Server at the conclusion of this installation.

    Click **Next**.

20. Click **Finish** to complete the installation.

21. Start the Identity Server to validate that the install completed successfully. Run the `start_ois_server` script, located under the *`ORACLE_HOME`*`/identity/oblix/apps/common/bin` directory to start the Identity Server on OAMHOST1, where *ORACLE_HOME* is the Identity Server install location.

7.3.1.2 Installing the Second Identity Server on OAMHOST2

Follow these steps to install the second Oracle Access Manager Identity Server on IDMHOST2:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Identity Server" chapter of the *Oracle Access Manager Installation Guide*.

2. Locate the Identity Server Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the Installers GUI console:

```
./Oracle_Access_Manager10_1_4_3_0_linux_Identity_Server -gui
```

3. On the Welcome to the InstallShield Wizard for Oracle Access Manager Identity Server screen, click **Next**.
4. Enter the username and group that the Identity Server will use. Specify `oracle/oinstall`.

   Click **Next**.
5. Specify the installation directory for Oracle Access Manager Identity Server. Specify the following value:

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

   Note: The base location for the Oracle Access Manager installation is `/u01/app/oracle/product/fmw/oam`. Oracle Access Manager components are installed in subdirectories automatically created by the installer under this location.

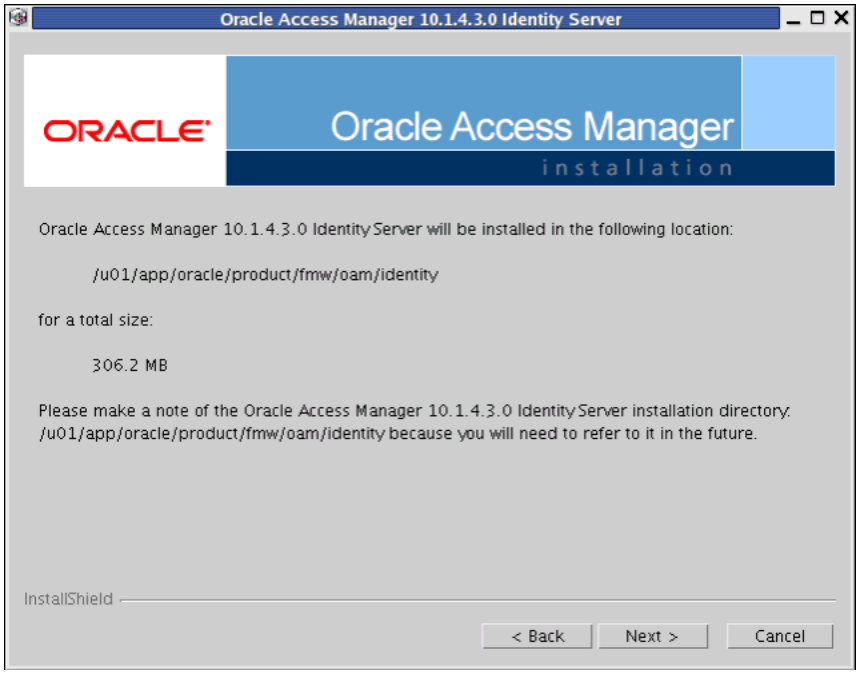
   The Identity Server is installed in the `identity` subdirectory created by the installer under the base location.

   The ORACLE_HOME location for the Oracle Access Manager Identity Server installation is:

   `/u01/app/oracle/product/fmw/oam/identity`

   Click **Next**.
6. Oracle Identity Manager will be installed in the following location (the `identity` directory is created by the installer automatically):

   `/u01/app/oracle/product/fmw/oam/identity`



7. Specify the location of the GCC runtime libraries, for example, `/home/oracle/oam_lib`.

   Click **Next**.

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

9. On the first Identity Server Configuration screen, specify the transport security mode between the WebPass/Identity client and the Identity Server. The choices are:

   - **Open Mode**: No encryption.
   - **Simple Mode**: Encryption through SSL and a Public Key Certificate provided by Oracle.
   - **Cert Mode**: Encryption through SSL and a Public Key Certificate provided by an external CA.

   Choose **Open Mode**.

   Click **Next**.

10. On the next Identity Server Configuration screen, specify the Identity Server ID, host name and port number for the Identity Server connection:

    - Enter a unique name for the Identity Server ID. For example: `IdentityServer_OAMHOST2`
    - Enter the hostname where the Identity Server will be installed. Make sure that the hostname can be resolved. For example: `oamhost2.mycompany.com`
    - Enter the port number on which this Identity Server communicates with its clients. For example, the default port number is 6022.

    Click **Next**.

11. On the next Identity Server Configuration screen, you are prompted whether this is the first Identity Server installation in the network for this LDAP directory server.

    Select **No**.

    Click **Next**.

12. On the next Identity Server Configuration screen, select the appropriate options if you want to set up SSL between the Identity Server and the Directory Server.

    - Directory Server hosting user data is in SSL
    - Directory Server hosting Oracle data is in SSL

    The enterprise deployment described in this manual does not use SSL for communication between components behind the firewall.

    Do not select anything.

    Click **Next**.

13. This displays the configuration screen. After the configuration is completed, the ReadMe file displays.

14. Review the Readme file.

    Click **Next** to display an installation summary.

15. The installation summary provides the details that you specified during this installation and instructs you to start the Identity Server at the conclusion of this installation.

    Click **Next**.

16. Click **Finish** to complete the installation.

17. Start the Identity Server to validate that the install completed successfully. Run the `start_ois_server` script, located under the *`ORACLE_HOME`*`/identity/oblix/apps/common/bin` directory to start the Identity Server on OAMHOST2, where *ORACLE_HOME* is the Identity Server install location.

7.3.2 Installing Oracle HTTP Server on OAMADMINHOST

This section describes how to install Oracle HTTP Server components on OAMADMINHOST.

7.3.2.1 Installing Oracle HTTP Server

Follow these steps to install Oracle HTTP Server on OAMADMINHOST:

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

2. Oracle HTTP Server is installed on port 7777 by default. Ensure that ports 7777, 8889, and 4443 are not in use by any service on OAMADMINHOST by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

   On UNIX:

   ```
   netstat -an | grep "7777"
   netstat -an | grep "8889"
   netstat -an | grep "4443"
   ```

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

   On UNIX:

   Remove the entries for ports 7777, 8889, and 4443 in the `/etc/services` file if the ports are in use by a service and restart the services, or restart the computer.

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

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

   ```
   #The http main port for ohs component
   OHS Port = 7777

   #This port indicates the OHS Proxy Port
   OHS Proxy Port = 8889

   #This port indicates the OHS SSL port
   OHS SSL Port = 4443
   ```

5. Start the Oracle Universal Installer for Oracle Fusion Middleware 11*g* Web Tier Utilities CD installation as follows:

   On UNIX, issue this command: `runInstaller`

   The `runInstaller` file is in the `../install/`*`platform`* directory where *platform* is a platform such as Linux or Solaris.

   The Specify Oracle Inventory screen is displayed.

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

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

   Operating System Group Name: `oinstall`

   A dialog box appears with the following message:

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

   Login as root and run the "/u01/app/oraInventory/createCentralInventory.sh"

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

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

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

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

8. On the Select Installation Type screen, select **Install and Configure**, and then click **Next**.

9. On the Prerequisite Checks screen, ensure that all the prerequisites are met, and then click **Next**.

10. On the Specify Installation Location screen set the location on OAMADMINHOST to:

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

    Click **Next**.

    Note: The ORACLE_HOME location for the Oracle HTTP Server install is `/u01/app/oracle/product/fmw/web`

11. On the Configure Components screen, select the following and deselect any other components:

- **Oracle HTTP Server**
- **Associate Selected Components with WebLogic Domain**

Click **Next**.

12. On the Specify WebLogic Domain screen, enter the location where you installed Oracle WebLogic Server. Note that the Administration Server must be running:
    - **Domain Host Name**: `idmhost1.mycompany.com`
    - **Domain Port No**: `7001`
    - **User Name**: `weblogic`
    - **Password**: `******`

    Click **Next**.
13. On the Specify Component Details screen, set the following values for OAMADMINHOST:
    - **Instance Home Location**:

      `/u01/app/oracle/admin/oamAdmin_ohs`

    - **Instance Name**: `oamAdmin_ohs`
    - **OHS Component Name**: `oamAdmin_ohs`

    Click **Next**.
14. On the Configure Ports screen, select **Specify Ports Using Configuration File**, and enter the full pathname to the staticports.ini file that you edited in the temporary directory.

    Click **Next**.
15. On the Email Address for Security Updates screen, specify these values:
    - **Email Address**: Provide the email address for your My Oracle Support account.
    - **Oracle Support Password**: Provide the password for your My Oracle Support account.
    - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

    Click **Next**.
16. On the Configuration Summary screen, ensure that the selections are correct and click **Install**.
17. On the Configuration screen, multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Configuration Completed screen appears.
18. On the Configuration Completed screen, click **Finish** to exit.

7.3.2.2 Validating the Installation of Oracle HTTP Server

Validate the installation of Oracle HTTP Server by following these steps:

1. Run the `opmnctl status` command from the *`INSTANCE_HOME`*`/bin` directory. For example:

   ```
   $ cd /u01/app/oracle/admin/oamAdmin_ohs
   ```

```
$ ./opmnctl status
Processes in Instance: oamAdmin_ohs
---------------------------------+--------------------+---------+---------
ias-component                    | process-type       |     pid | status
---------------------------------+--------------------+---------+---------
oamAdmin_ohs                     | OHS                |   28575 | Alive
```

2. Open a web browser and go to the URL `http://`*`hostname`*`.mycompany.com:`*`port`* to view the default Oracle HTTP Server Home page. For example:

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

7.3.3 Installing WebPass on OAMADMINHOST

Follow these steps to install WebPass for Oracle Access Manager on OAMADMINHOST:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing WebPass" chapter of the *Oracle Access Manager Installation Guide*.
2. Locate the WebPass Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console:

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebPass -gui
   ```

3. On the Welcome to the InstallShield Wizard for Oracle Access Manager 10.1.4.3.0 WebPass screen, click **Next**.
4. On the Customer Information screen, enter the username and group that the Identity Server will use. The default value for username and group is `nobody`. For example, enter `oracle/oinstall`.

   Click **Next**.
5. Specify the installation directory for Oracle Access Manager WebPass. For example, enter:

   ```
   /u01/app/oracle/product/fmw/oam/webcomponents
   ```

   Click **Next**.

Note: The base location for the Oracle Access Manager Web components installation is `/u01/app/oracle/product/fmw/oam/webcomponents`. The Oracle Access Manager Web components are installed in subdirectories automatically created by the installer under this location.

WebPass is installed in the `identity` subdirectory created by the installer under the base location.

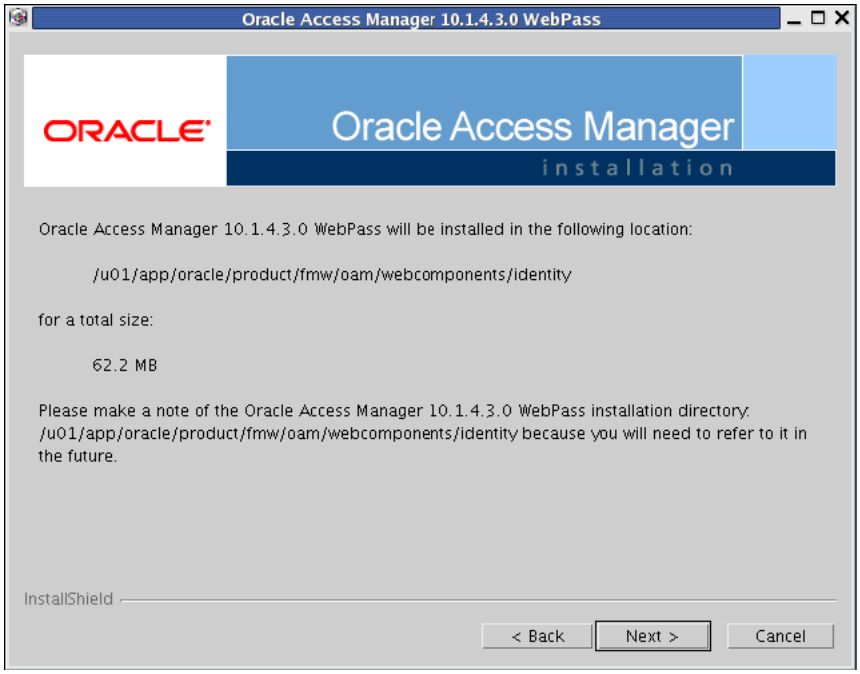
The ORACLE_HOME location for the Oracle Access Manager WebPass installation is:

```
/u01/app/oracle/product/fmw/oam/webcomponents/identi
ty
```

---

6. Oracle Access Manager 10.1.4.3 WebPass will be installed in the following directory:

   `/u01/app/oracle/product/fmw/oam/webcomponents/identity`



7. On the Oracle Access Manager WebPass Configuration screen, specify the location of the GCC runtime libraries. For example: `/home/oracle/oam_lib`

   Click **Next**.

8. The Installing Oracle Access Manager WebPass screen appears.

9. When the WebPass Configuration screen appears, specify the Transport Security Protocol between the WebPass/Identity client and the Identity Server. Make sure to choose the same protocol as you did for the Identity Server. Select **Open Mode**.

   Click **Next**.

10. The next screen in the WebPass Configuration series appears. Specify the WebPass ID, host name and port number for the Identity Server connection:

    - Enter a unique name for this WebPass ID. For example: `WebPass_OAMADMINHOST`
    - Enter the hostname of the Identity Server with which this WebPass should communicate. For example: `oamhost1.mycompany.com`
    - Enter the port number of the Identity Server with which this WebPass should communicate. For example, the default port number is 6022.

    Click **Next**.

11. Oracle Access Manager WebPass is installed under your Oracle Access Manager WebPass installation directory. In order to use the Oracle Access Manager WebPass module, configure your web server by modifying the configuration in your web server directory.

    Select **Yes** when the **Proceed with Automatic update of httpd.conf?** question appears.

    Click **Next**.

12. Enter the absolute path of `httpd.conf` in your Web Server `config` directory. The absolute path of the httpd.conf file is:

    `/u01/app/oracle/admin/`*`instanceName`*`/config/OHS/`*`componentName`*`/httpd.conf`

    For example:

    `/u01/app/oracle/admin/oamAdmin_ohs/config/OHS/oamAdmin_ohs/httpd.conf`

    Click **Next**.

13. A screen displays that advises you that if the web server is set up in SSL mode, then the `httpd.conf` file needs to be configured with the SSL parameters.

    To manually tune your SSL configuration, follow the instructions that are displayed.

    Click **Next**.

14. A screen displays that advises you that information on the rest of the product setup and your web server configuration is available in the document: *`documentLocation`*. The screen asks you whether you would like the installer to launch a browser to view the document.

    Select **No**, then click **Next**.

15. A screen displays that advises you to launch a browser and open the *documentLocation* document for further information on configuring your web server.

    Click **Next**.

16. On the Coreid 10.1.4.3.0 ReadMe screen, click **Next**.

17. The installation summary provides the details that you specified during this installation and instructs you to start the Identity Server at the conclusion of this installation. Click **Next**.

18. Click **Finish** to complete the installation.

7.3.3.1 Configuring Oracle HTTP Server and WebPass Communication

To establish communication between WebPass and its Identity Server, follow these steps:

1. Stop the WebPass Web server instance:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   ```

2. Update the *OHS_INSTANCE_HOME*/config/OPMN/opmn/opmn/opmn.xml file to set the environment variable LD_ASSUME_KERNEL for the OHS1 component, as shown in this example:

   ```
   ...
   <ias-component id="oamAdmin_ohs">
       <process-type id="OHS" module-id="OHS1">
           <environment>
               <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
           </environment>
           <module_data>
   ...
   ```

3. Stop and then start Identity Server on OAMHOST1 and OAMHOST2:

   ```
   ORACLE_HOME/identity/oblix/apps/common/bin/restart_ois_server
   ```

   where *ORACLE_HOME* refers to the location where the Identity Server is installed.

4. Start the WebPass Web server instance:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

7.3.3.2 Validating the WebPass Installation

Follow these steps to validate the WebPass installation:

1. To make sure that your Identity Server and WebPass Web server are running, navigate to the Identity System Console by specifying the following URL in your web browser:

   ```
   http://hostname:port/identity/oblix
   ```

   where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   ```
   http://oamadminhost.mycompany.com:7777/identity/oblix
   ```

2. The Identity System landing page should appear.

   Do not select any link on the Identity System landing page because the system has not yet been set up.

7.3.4 Configuring Identity Servers Using WebPass

This section describes how to configure the Identity Servers on OAMHOST1 and OAMHOST2 using WebPass.

7.3.4.1 Configuring the First Identity Server

After the Identity Server and the WebPass instance are installed, you must specify the associations between them to make the system functional. Follow these steps to configure the first Identity Server:

1. Navigate to the Identity System Console by specifying the following URL in your web browser:

   `http://`*`hostname:port`*`/identity/oblix`

   where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/identity/oblix`

   Click the **Identity System Console** link.

2. On the **System Console Application is not set up** page, click the **Setup** button.

3. On the **Product Setup page**, specify your user data directory server type. Select **Oracle Virtual Directory** or **Oracle Internet Directory** based on how your environment is configured.

   Click **Next**.

4. On the **Schema Change** page, click **Next**. You do not need to do anything because the schema was updated during Identity Server installation.

5. Specify the user data directory details based on your installation:

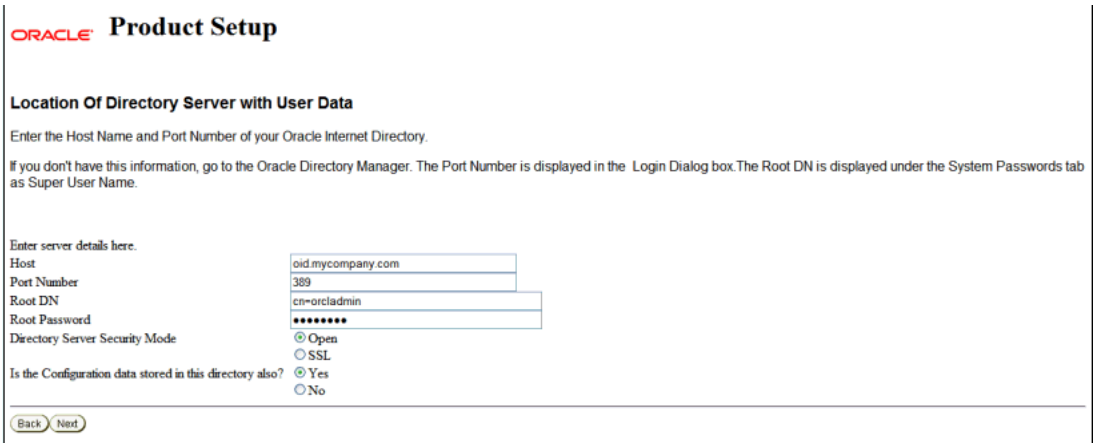
   - **Host**: The DNS host name of the user data directory server. Enter:

     `oid.mycompany.com` (if your user store is in Oracle Internet Directory)

     `ovd.mycompany.com` (if your user store is in Oracle Virtual Directory)

   - **Port Number**: The port of the user data directory server. For example: `389`
   - **Root DN**: The bind distinguished name of the user data directory server. For example: `cn=orcladmin`
   - **Root Password**: The password for the bind distinguished name.
   - **Directory Server Security Mode**: Open or SSL-enabled between the user data directory server and Identity Server. Select **Open**.
   - **Is Configuration data stored in this directory also?**: `Yes` (default)

   Click **Next**.



6. On the **Location of Configuration Data and the Oracle Access Manager Searchbase** page, specify the distinguished name (DN) for the configuration data and the searchbase for user data. The configuration DN is the directory tree where Oracle Access Manager stores its configuration data. The searchbase is the node in the directory tree where the user data is stored and is usually the highest base for all user searches.

   When the user data and configuration data are in the same directory, the entries can be specified as follows:

   - **Configuration DN**: `dc=us,dc=mycompany,dc=com`
   - **Searchbase**: `dc=us,dc=mycompany,dc=com`

   Click **Next**.

   > **Note:** The configuration DN for the Oracle Access Manager Identity Server and the Oracle Access Manager Access Server must be the same. Also, if the configuration data and the search data are in different directories they should have unique DNs and the searchbase cannot be `o=Oblix, configurationDN` or `ou=Oblix, configurationDN`.

7. On the Person Object Class screen, specify the Person object class for the User Manager as shown below:

   Person Object Class: *inetorgPerson*

   Click the **Auto configure objectclass** text box.

   Click **Next**.

   > **Note:** The person object class specified during this setup is the person object class used by the User Manager application.

8. On the Group Object Class screen, specify the Group object class as shown below. For example, the Group object class would be an entry resembling the following:

   Group Object Class: *GroupofUniqueNames*

   Click the **Auto configure objectclass** text box.

Click **Next**.

Note: The group object class specified during this setup is the only group object class used by the Group Manager application.

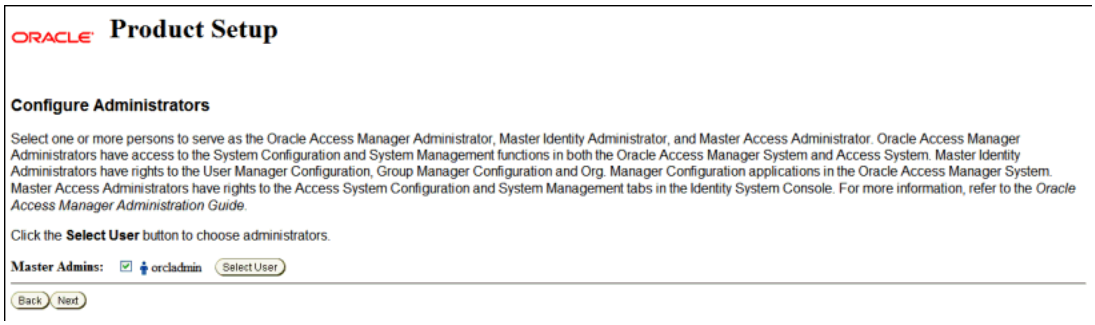
---

9. Stop the WebPass Web server instance on OAMADMINHOST.
10. Stop and then start the Identity Servers on OAMHOST1 and OAMHOST2.
11. Start the WebPass Web server instance on OAMADMINHOST.
12. In the Return to the Oracle Access Manager Product Setup window, click **Next**.
13. A screen appears summarizing the person object class changes that were made automatically with the following question: "Is the following configuration correct for the objectclass 'inetorgperson'?

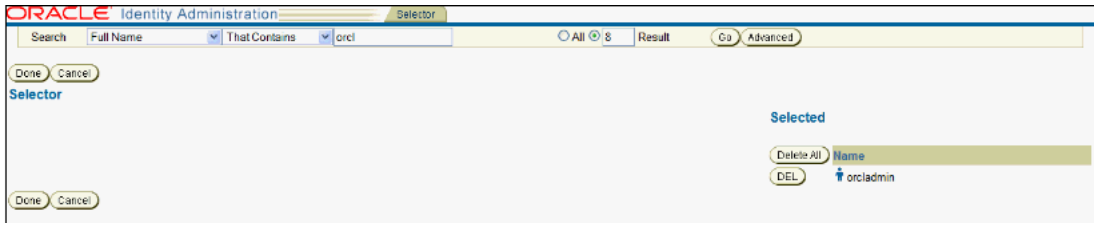
    Review the Person object class attributes and then click **Yes**.

    Review the Group object class attributes and then click **Yes**.
14. A screen appears summarizing the group object class changes that were made automatically with the following question: "Is the following configuration correct for the objectclass 'groupOfUniqueNames'?

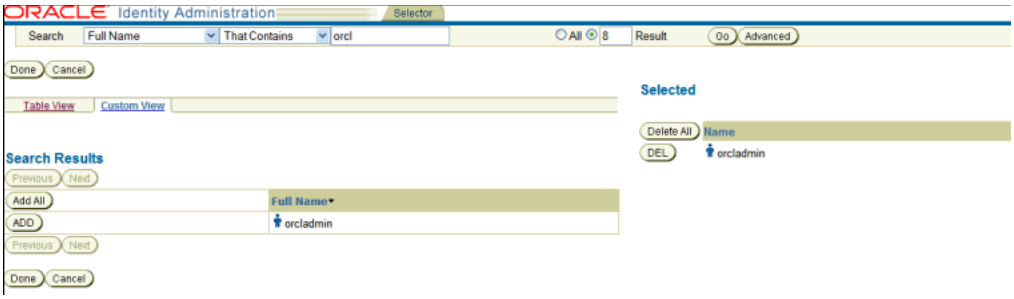
    Review the Group object class attributes and then click **Yes**.
15. On the **Configure Administrators** page, the user `orcladmin` is configured as the Master Administrator by default. If you do not want to add any additional Administrator users, click **Next**.



To add additional users as administrators, click the **Select User** button to bring up the Selector page.



On the **Selector** page, complete the fields with the search criteria for the user you want to select as an administrator and click **Go**. A minimum of three characters is required to return search results.



16. Search results matching the specified criteria appear.

    Click **Add** next to the person you want to select as an administrator.

17. The name of the person appears under the **Selected** column on the right.

    Add other names as needed.

    Click **Done**.

18. On the **Configure Administrators** page, view the selected users listed as administrators.

    Click **Next**.

19. On the **Securing Data Directories** page, click **Done** to complete the Identity System setup.

20. Verify the configuration by performing these steps:

    a. Access the Oracle Access Manager system console at this URL:

    `http://OAMADMINHOST:`*`port`*`/identity/oblix`

    where *port* is the Oracle HTTP Server port.

    For example, enter the following URL in your web browser:

    `http://oamadminhost.mycompany.com:7777/identity/oblix`

    b. Click User Manager, Group Manager, or Org. Manager and log in with the newly created administrator user's credentials.

7.3.4.2 Configuring the Second Identity Server

Follow these steps to configure the second Identity Server:

1. Navigate to the Identity System Console by specifying the following URL in your web browser:

   `http://`*`hostname:port`*`/identity/oblix`

   where *hostname* refers to computer that hosts the WebPass Web server and `port` refers to the HTTP port number of the WebPass Web server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/identity/oblix`

   Click the **Identity System Console** link.

2. A login dialog box appears.

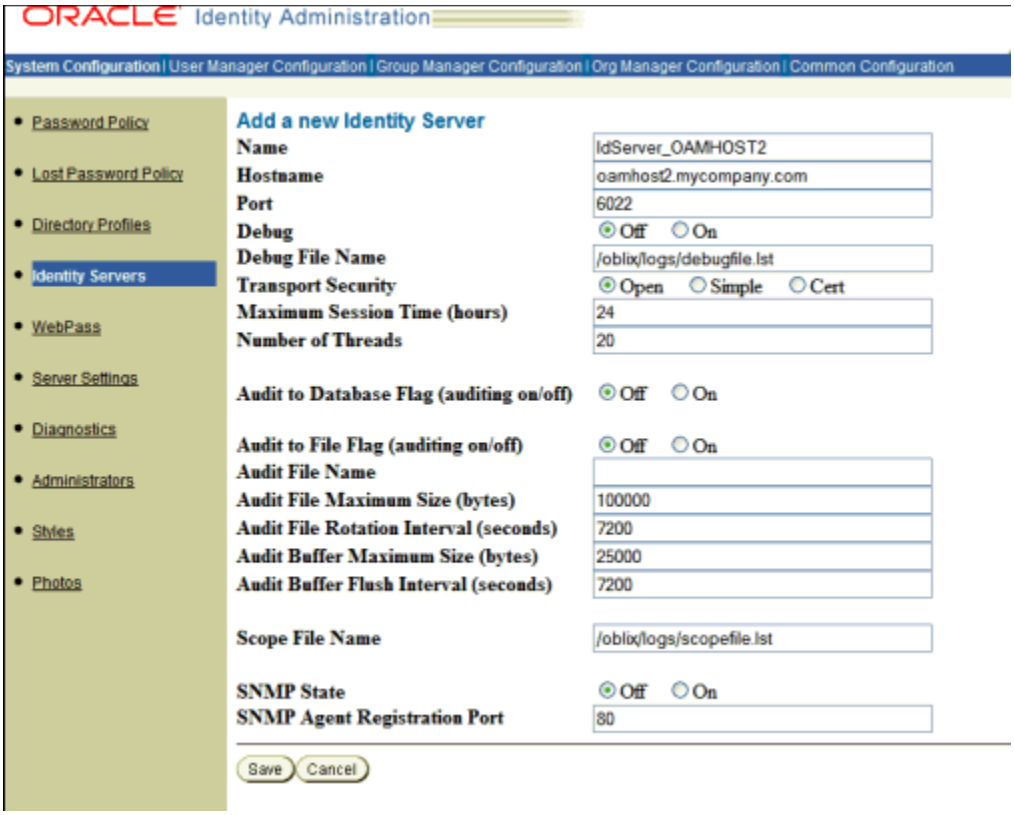
   Provide the administrator user name and password.

Click **Login**.

3. On the System Configuration screen, click the **Identity System Console** and select **System Configuration > Identity Servers**.
4. Click **Add** and specify the values shown below on the Add a new Identity Server screen:
   - **Name**: `idserver_oamhost2`
   - **Hostname**: `oamhost2.mycompany.com`
   - **Port**: `6022`
   - **Debug**: `Off`
   - **Debug File Name**: `/oblix/logs/debugfile.lst`
   - **Transport Security**: `Open`

   Accept the default values for the remaining parameters, unless required in your environment:

   - **Maximum Session Time (hours)**: `24` (default)
   - **Number of Threads**: `20` (default)
   - **Audit to Database Flag (auditing on/off)**: `Off` (default)
   - **Audit to File Flag (auditing on/off)**: `Off` (default)
   - **Audit File Name**: Leave blank (default)
   - **Audit File Maximum Size (bytes)**: `100000` (default)
   - **Audit File Rotation Interval (seconds)**: `7200` (default)
   - **Audit Buffer Maximum Size (bytes)**: `25000` (default)
   - **Audit Buffer Flush Interval (seconds)**: `7200` (default)
   - **Scope File Name**: `/oblix/logs/scopefile.lst` (default)
   - **SNMP State**: `Off` (default)
   - **SNMP Agent Registration Port**: `80` (default)



5. Click the Identity System Console and select **System Configuration > WebPass**.
6. The OAMWebPass_OAMADMINHOST instance is listed.

   Click the WebPass instance for OAMADMINHOST.
7. On the Details for WebPass screen, click **List COREid Servers**.
8. The Identity Servers associated with the WebPass are listed.

   Click **Add**.
9. On the Add a new Identity Server to the WebPass screen:

   Select the identity server installed on OAMHOST2.

   Select **Primary Server** and specify **2** connections.

   Click **Add**.

This completes the configuration of the Identity System.

You can now begin the installation of the Access System, which includes the Policy Manager, Access Server, and WebGate components.

7.4 Access System Installation and Configuration

This section provides details about the Access System installation and configuration. Access System components include the Policy Manager, Access Server, and WebGate components.

7.4.1 Installing the Policy Manager on OAMADMINHOST

The first step in installing the Access System is to install and configure the Policy Manager.

The Oracle Access Manager Policy Manager can be installed directly.

The Policy Manager must be installed in the same base directory as WebPass on OAMADMINHOST.

To install the Policy Manager, follow these steps:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Policy Manager" chapter of the *Oracle Access Manager Installation Guide*.
2. Locate the Policy Manager Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console.

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_PolicyManager -gui
   ```

3. On the Welcome to the InstallShield Wizard for Oracle Access Manager Policy Manager screen, click **Next**.
4. On the Customer Information screen, enter the username and group that the Identity Server will use. The default value for username and group is `nobody`. For example, enter `oracle/oinstall`.

   Click **Next**.
5. You are prompted for the installation directory.

   Specify the directory where you installed WebPass, for example:

   ```
   /u01/app/oracle/product/fmw/oam/webcomponents
   ```

   Click **Next**.

   Note: The base location for the Oracle Access Manager WebPass and Policy Manager installations is `/u01/app/oracle/product/fmw/oam/webcomponents`. The WebPass and Policy Manager components are installed in subdirectories automatically created by the installer under this location.

   The Policy Manager is installed in the `access` subdirectory created by the installer under the base location.

   The ORACLE_HOME location for the Oracle Access Manager Policy Manager Server installation is:

   ```
   /u01/app/oracle/product/fmw/oam/webcomponents/access
   ```

   ---

6. Oracle Access Manager Policy Manager will be installed in the following directory:

   ```
   /u01/app/oracle/product/fmw/oam/webcomponents/access
   ```

7. Specify the location of the GCC runtime libraries. For example, specify: `/home/oracle/oam_lib`.

   Click **Next**.

8. A progress message appears, then the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

   Select **Oracle Internet Directory**.

9. You are prompted to specify whether policy data is in a separate directory server than the directory containing Oracle configuration data or user data, and if so, whether you would like the installer to automatically configure the directory server containing policy data.

   Select **No**.

   Click **Next**.

10. On the Configure Access Manager for using SSL mode with Directory Server screen, you are prompted for the communication method for Oracle Internet Directory.

    These three options appear:

    - Directory Server hosting user data is in SSL
    - Directory Server hosting Oracle data is in SSL
    - Directory Server hosting Policy data is in SSL

    Do not select any of these options. Click **Next**.

11. On the Policy Manager Configure screen, you are asked to specify the transport security mode between this Access Manager and Access Servers that you plan to install in the future.

    Choose **Open Mode**.

    Click **Next**.

12. On the Configure Web Server screen, select **Yes** for the **Proceed with automatic updates of httpd.conf?** option.

    Click **Next**.

13. Specify the full path of the directory containing the `httpd.conf` file. The path defaults to the `httpd.conf` file location for the Oracle HTTP Server installed on OAMADMINHOST.

    Click **Next**.

    A message informs you that the Web Server Configuration has been modified for Policy Manager.

14. A screen displays that advises you that if the web server is set up in SSL mode, then the `httpd.conf` file needs to be configured with the SSL parameters.

    To manually tune your SSL configuration, follow the instructions that are displayed.

    Click **Next**.

15. A screen displays that advises you that information on the rest of the product setup and your web server configuration is available in the document: *`documentLocation`*. The screen asks you whether you would like the installer to launch a browser to view the document.

    Select **No**, then click **Next**.

16. A screen displays that advises you to launch a browser and open the *`documentLocation`* document for further information on configuring your web server.

    Click **Next**.

17. On the Coreid 10.1.4.3.0 ReadMe screen, click **Next**.

18. A message appears informing you that the installation was successful.

    Click **Finish**.

19. Stop and start the Oracle HTTP Server installed on OAMADMINHOST using the `opmnctl` commands shown below:

    ```
    ORACLE_INSTANCE/bin/ opmnctl stopproc ias-component=ohs1

    ORACLE_INSTANCE/bin/opmnctl startproc ias-component=ohs1
    ```

20. Stop and start the Identity Server installed on OAMHOST1 and OAMHOST2 using these commands:

    ```
    ORACLE_HOME/identity/oblix/apps/common/bin/stop_ois_server

    ORACLE_HOME/identity/oblix/apps/common/bin/start_ois_server
    ```

    where *ORACLE_HOME* refers to the directory where the Identity Server is installed.

21. Validate that the Policy Manager installation was successful by opening a web browser and bringing up the Policy Manager Home page:

    ```
    http://oamadminhost.mycompany.com:7777/access/oblix
    ```

7.4.1.1 Configuring the Policy Manager

The Policy Manager must be configured to communicate with Oracle Internet Directory. Follow these steps to configure the communication:

1. Make sure your Web server is running.
2. Navigate to the Access System Console by specifying the following URL in your web browser:

   `http://`*`hostname:port`*`/access/oblix`

   where *hostname* refers to the host where the Policy Manager Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

   Note: The WebPass and Policy Manager components share the same Oracle HTTP Server instance on OAMADMINHOST.

3. Click the **Access System Console** link.

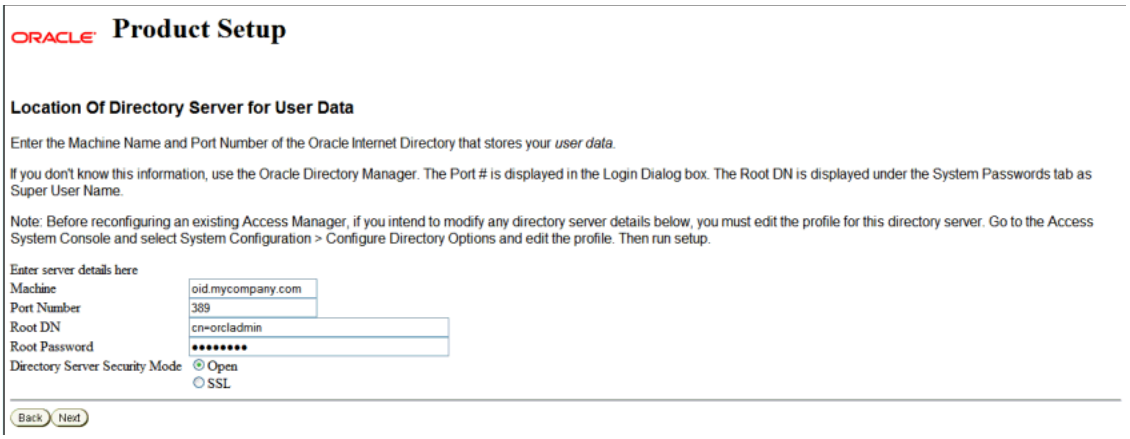
   A message informs you that the Administration Console Application is not yet set up.
4. Click the **Setup** button.
5. You are prompted for the User Directory Server Type.

   If you are using Oracle Virtual Directory, choose **Data Anywhere** and if you are using Oracle Internet Directory, choose **Oracle Internet Directory**.
6. On the Location of Directory Server for User Data screen, specify the following server details:
   - **Machine**: Specify the DNS host name of the user data directory server. Enter:

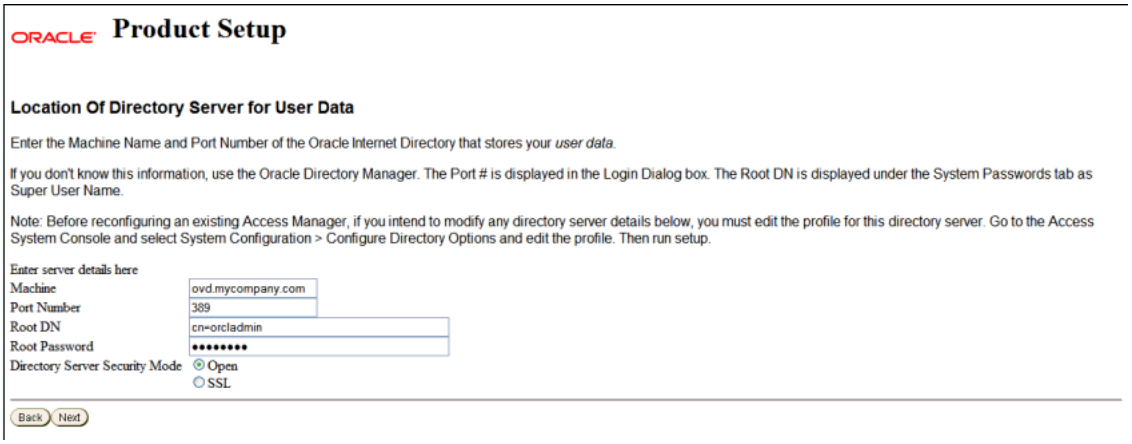
     `oid.mycompany.com` (if your user store is in Oracle Internet Directory)

     `ovd.mycompany.com` (if your user store is in Oracle Virtual Directory)
   - **Port Number**: Specify the port of the user data directory server. Enter the non-SSL port for the directory server. For example: `389`
   - **Root DN**: Specify the bind DN (distinguished name) for the user data directory server. For example: `cn=orcladmin`
   - **Root Password**: Specify the password for the bind distinguished name.
   - **Directory Server Security Mode**: Select **Open**.

   This screen capture shows the values for the Location of Directory Server for User Data screen if your user store is Oracle Internet Directory:



This screen capture shows the values for the Location of Directory Server for User Data screen if your user store is Oracle Virtual Directory:



Click **Next**.

7. On the Directory Server Type containing Configuration Data screen, choose **Oracle Internet Directory**.

   Click **Next**.

8. On the Directory Server containing User Data and Directory Server containing Configuration Data screen, a message informs you that the user data and configuration data can be stored in either the same or different directories.

   Select **Store Configuration Data in the User Directory Server**.

   Click **Next**.

9. On the Directory Server containing User Data and Directory Server containing Policy Data screen, a message informs you that the user data and policy data can be stored in either the same or different directories.

   Select **Store Policy Data in the User Directory Server**.

10. On the Location of the Oracle Access Manager Configuration data, the Searchbase, and the Policybase screen, specify the appropriate information for your installation. For example:

- **Searchbase**: `dc=us,dc=mycompany,dc=com` (This must be the same searchbase you specified during Identity Server configuration)
- **Configuration DN**: `dc=us,dc=mycompany,dc=com` (This must be the same configuration DN you specified during Identity Server configuration)
- **Policy Base**: `dc=us,dc=mycompany,dc=com`

Click **Next**.

11. On the Person Object Class screen, specify the Person object class that was specified during Identity Server system configuration:

    Person Object Class: *inetorgperson*

    Click **Next**.

12. You are prompted to restart the Web server. The Identity Servers must be restarted, along with the Web Server instance. Follow the sequence shown below:

    a. Stop the Oracle HTTP Server on OAMADMINHOST.

    b. Restart the Identity Server on OAMHOST1 and OAMHOST2.

    c. Start the Oracle HTTP Server on OAMADMINHOST.

    Click **Next**.

13. On the Root Directory for the Policy Domains screen, specify the root directory for policy domains.

    Accept the default root directory for policy domains, for example:

    Policy Domain Root: /

    Click **Next**.

14. On the Configuring Authentication Schemes screen, select Yes to automatically configure authentication schemes.

    Click **Next**.

15. On the next screen, select both **Basic Over LDAP** and **Client Certification authentication schemes**.

    Click **Next**.

16. On the Define a new authentication scheme screen, specify the Basic over LDAP parameters. The values on the screen are prefilled. Review the parameters. Change the parameter values, if required by your environment:

    - **Name**: `Basic Over LDAP`
    - **Description**: `This scheme is Basic over LDAP, using the built-in browser login mechanism`
    - **Level**: `1`
    - **Challenge Method**: `Basic`
    - **Challenge Parameter**: `realm: LDAP User Name/Password`
    - **Plugin**(s):
      - **Plugin Name**: `credential_mapping`

        Plugin Parameters:

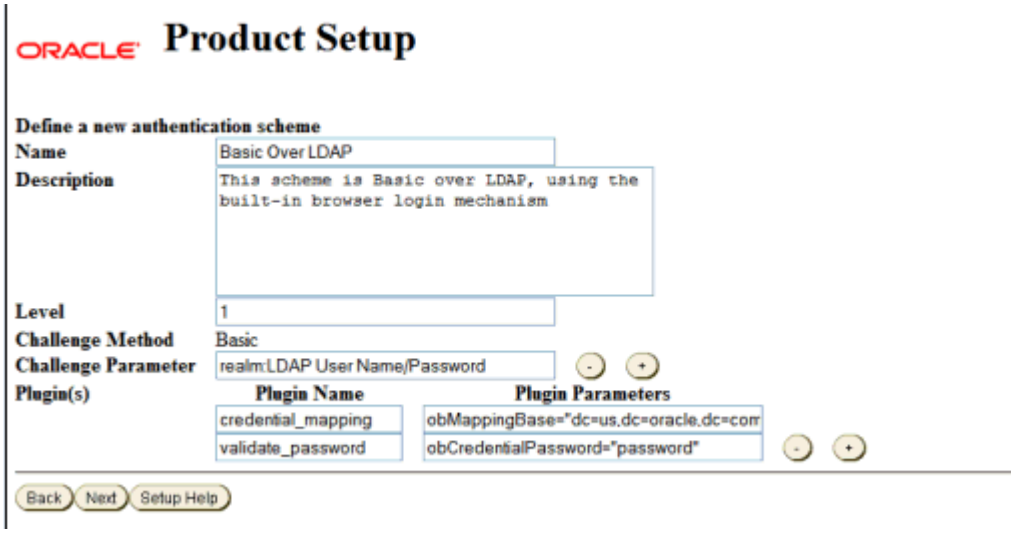
        ```
        obMappingBase="dc=us,dc=mycompany,dc=com",
        obMappingFilter="(&(objectclass=inetorgperson)
        ```

```
(uid=%userid%))"
```

- **Plugin Name**: `validate_password`

  Plugin Parameters: `obCredentialPassword="password"`

Click **Next**.



17. On the next Define a new authentication scheme screen, specify the Client Certificate parameters. The values on the screen are prefilled. Review the parameters. Change the parameter values, if required by your environment.

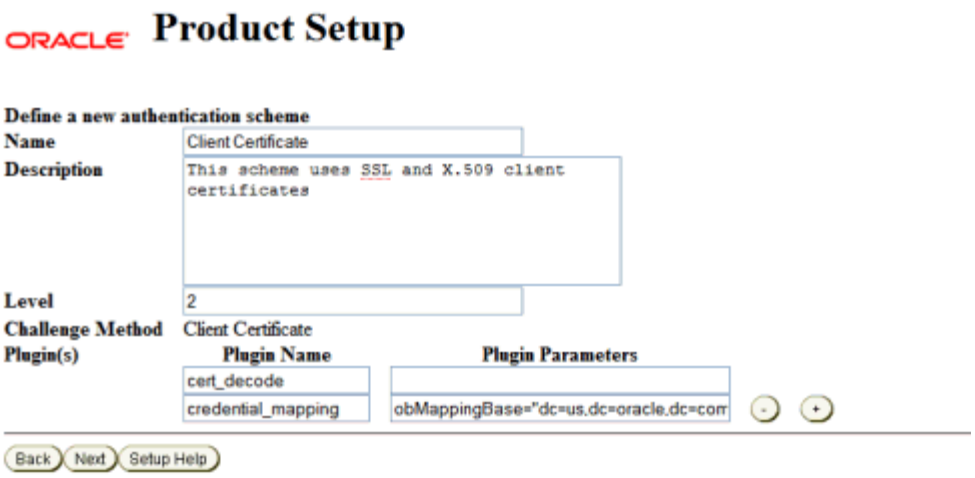
    - **Name**: `Client Certificate`
    - **Description**: `This scheme uses SSL and X.509 client certificates`
    - **Level**: `2`
    - **Challenge Method**: `Client Certificate`
    - **Challenge Parameter**: `realm: LDAP User Name/Password`
    - **Plugin**(s):
      - **Plugin Name**: `cert_decode`

        Plugin Parameters:
      - **Plugin Name**: `credential_mapping`

        Plugin Parameters:

        ```
        obMappingBase="dc=us,dc=mycompany,dc=com",
        obMappingFilter="(&(objectclass=inetorgperson)
        (mail=%certSubject.E%))"
        ```

    Click **Next**.



18. On the Configure Policies to Protect NetPoint Identity System and Access Manager screen, select **Yes** to configure policies to protect Access System related URLs.

    Click **Next**.

19. On the next page, instructions for Securing Data Directories and Configuring Identity and Access policy domains are shown. Review the instructions to complete the tasks and then restart the Identity Servers and web server instances by following the steps below:

    a. Stop the WebPass/Policy Manager Web server instance on OAMADMINHOST.

    b. Stop and then start the Identity Servers on OAMHOST1 and OAMHOST2.

    c. Start the WebPass/Policy Manager Web server instance on OAMADMINHOST.

    Verify that all the processes are back up again and then click **Done**.

20. The Policy Manager home page appears.

    Confirm that the Policy Manager is installed correctly by performing the following steps:

    a. Navigate to the Access System Console from your browser. For example:

    `http://hostname:port/access/oblix`

    where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

    For example, enter the following URL in your web browser:

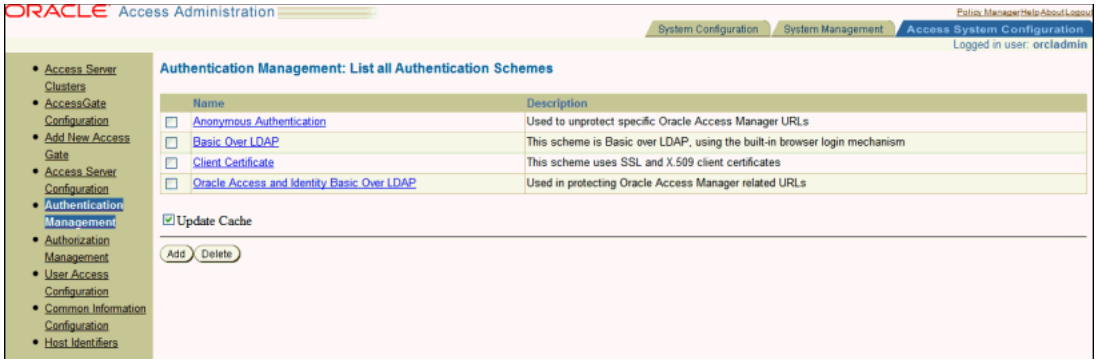
    `http://oamadminhost.mycompany.com:7777/access/oblix`

    b. Select the **Access System Console** link.

    c. Log in as an administrator.

    d. Select the **Access System Configuration** tab, then click **Authentication Management** when it appears in the left column.

A list of the authentication schemes configured appears.



7.4.2 Installing the Access Server on OAMHOST1 and OAMHOST2

The second step in installing the Access System is to install the Access Server.

Before you begin installing the Access Server, you need to create an instance for it within the Access system Console.

7.4.2.1 Creating an Access Server Instance

Follow these steps to create an Access Server instance:

1. Log into the Access System Console by specifying the following URL in your web browser:

   `http://hostname:port/access/oblix`

   where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

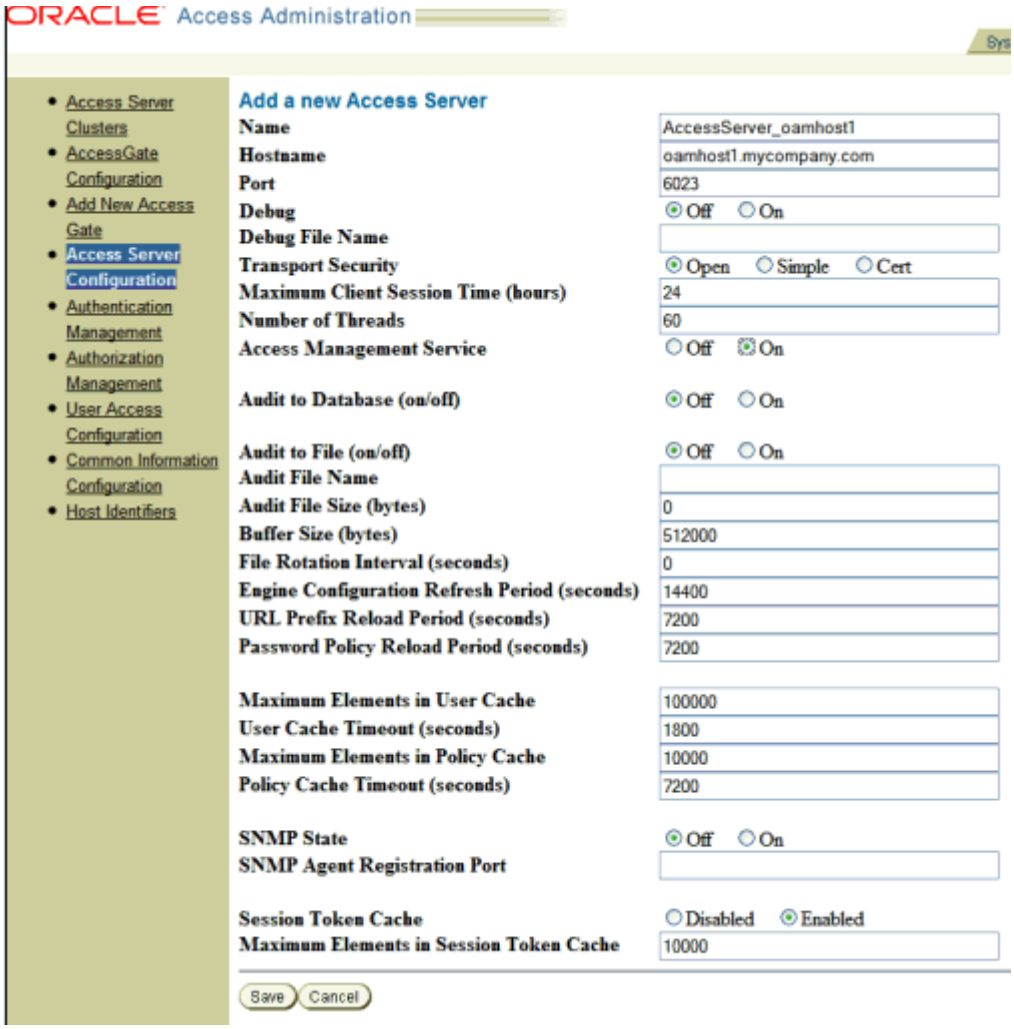
   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. On the Access System main page, click the **Access System Console** link, then log in as the administrator.
3. Click the **Access System Configuration** tab, then click **Access Server Configuration** when the side navigation bar appears.
4. Click **Add** to display the **Add Access Server** page with some defaults.
5. Specify the parameters shown below for the Access Server you plan to install:
   - **Name**: Descriptive name for the Access Server that is different from any others already in use on this directory server. For example: `AccessServer_OAMHOST1`
   - **Hostname**: Name of the computer where the Access Server will be installed. The Access Server does not require a Web server instance. For example: `oamhost1.mycompany.com`
   - **Port**: Port on which the Access Server will listen. For example: `6023`
   - **Transport Security**: Transport security between all Access Servers and associated WebGates must match. Specify **Open**.

- **Access Management Service**: This should be enabled only if the WebGate is using the Policy Manager API. In this case, select **ON**, since the WebGate will be using the PolicyManager API.

Review the remaining prefilled default values. Modify these values, if required by your environment.

Click **Save**.



6. The **Access Server Configuration: List All Access Servers** page appears with a link to this instance. Verify that the Access Server has been created with the correct values by clicking on the link for the Access Server just created.
7. Repeat steps 3 through 6 for each additional Access Server you want to install. Substitute values where appropriate. For example, when creating the second Access Server instance, specify the following values:
   - **Name**: `AccessServer_OAMHOST2`
   - **Hostname**: `oamhost2.mycompany.com`
8. Click **Logout** and then close the browser window.

7.4.2.2 Starting the Access Server Installation

Follow these steps to start the Access Server installation:

1. Locate the AccessServer Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console. Log in as a user with Administrator privileges.

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_Access_Server -gui
   ```

2. On the Welcome to the InstallShield Wizard for Oracle Access Manager Access Server screen, click **Next**.

3. On the Customer Information screen, enter the username and group that the Identity Server will use. The default value for username and group is `nobody`. For example, enter `oracle/oinstall`.

   Click **Next**.

4. Specify the installation directory for Oracle Access Manager Access Server. For example, enter:

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

   Note: The base location for the Oracle Access Manager Access Server installation is `/u01/app/oracle/product/fmw/oam`. Oracle Access Manager components are installed in subdirectories automatically created by the installer under this location.

   The Access Server is installed in the `access` subdirectory created by the installer under the base location.

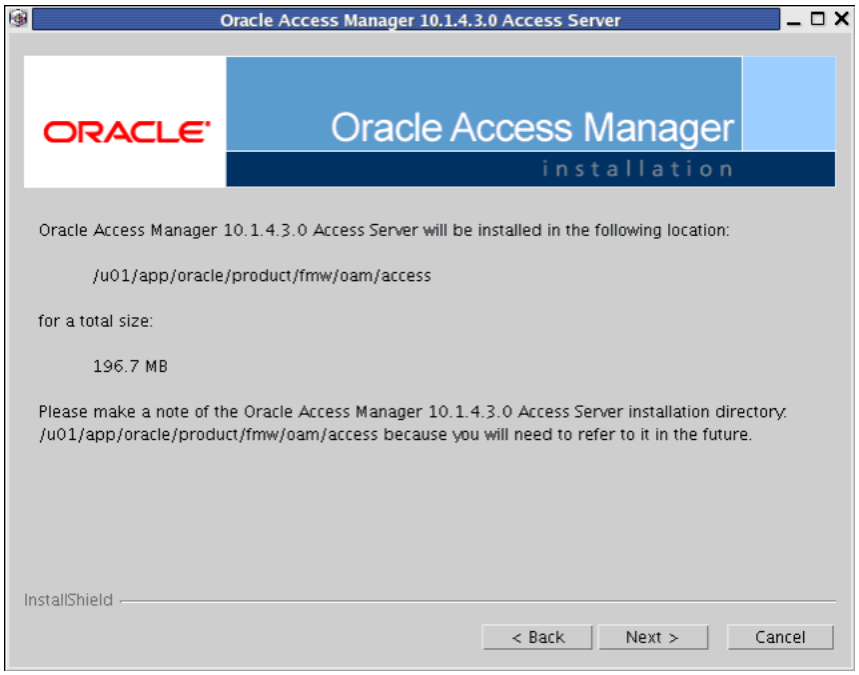
   The ORACLE_HOME location for the Oracle Access Manager Access Server installation is:

   ```
   /u01/app/oracle/product/fmw/oam/access
   ```

   Click **Next**.

5. Oracle Access Manager Access Server will be installed in the following location (the `access` directory is created by the installer automatically):

   ```
   /u01/app/oracle/product/fmw/oam/access
   ```



Click **Next**.

6. Specify the location of the GCC runtime libraries. For example: `/home/oracle/oam_lib`.

   Click **Next**.

   The installation progress screen is shown. After the installation process completes, the Access Server Configuration screen appears.

7. On the Access Server Configuration screen, you are prompted for the transport security mode.

   Specify the transport security mode. The transport security between all Access System components (Policy Manager, Access Servers, and associated WebGates) must match. Select one of the following: **Open Mode**, **Simple Mode**, or **Cert Mode**.

   Select **Open Mode**.

   Click **Next**.

8. On the next Access Server Configuration screen, you are prompted for the mode in which the Directory Server containing Oracle configuration data is running.

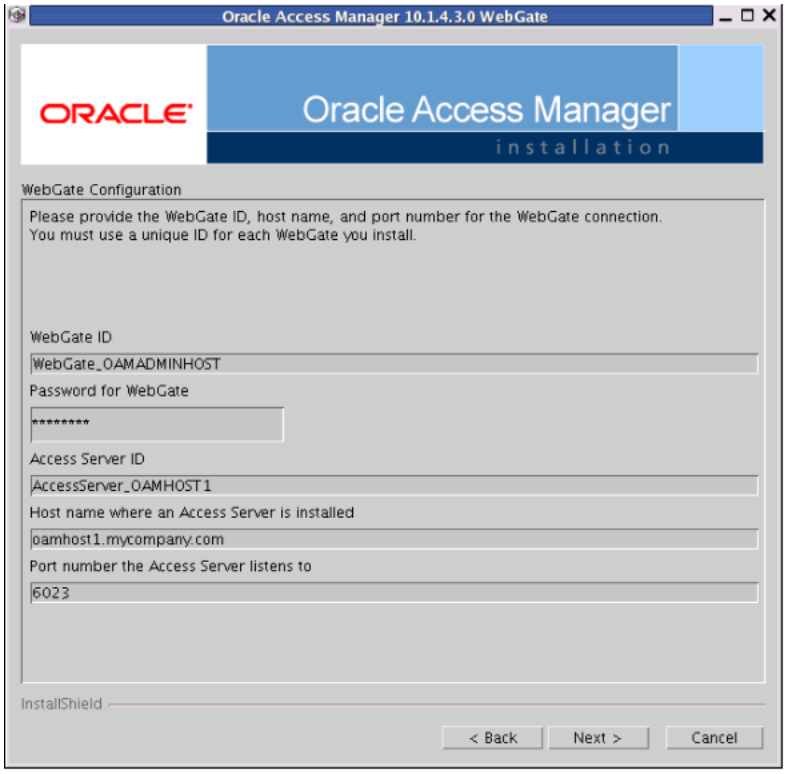
   Select **Open**. This is the default choice.

   On the same screen, specify the following directory server details:

   - **Host**: Specify the DNS hostname of the Oracle configuration data directory server. For example: `oid.mycompany.com`
   - **Port Number**: Specify the port of the Oracle configuration data directory server. For example: `389` (OID non-SSL Port)
   - **Root DN**: Specify the bind distinguished name of the Oracle configuration data directory server. For example: `cn=orcladmin`
   - **Root Password**: Specify the password for the bind distinguished name.

- **Type of the Directory Server containing Oracle configuration data**: Select **Oracle Internet Directory**.

Click **Next**.



9. On the next Access Server Configuration screen, specify where the Oracle Access Manager Policy data is stored. Select **Oracle Directory** and click **Next**.
10. On the next Access Server Configuration screen, specify the Access Server ID, the Configuration DN and the Policy Base specified when creating the Access Server instances in Section 7.4.2.1, "Creating an Access Server Instance."

    Enter the requested details, for example:

    - **Access Server ID**: `AccessServer_OAMHOST1`
    - **Configuration DN**: `dc=us,dc=mycompany,dc=com`
    - **Policy Base**: `dc=us,dc=mycompany,dc=com`

11. Review the information on the Oracle COREId 10.1.4.3 ReadMe screen.

    Click **Next**.

12. A message appears informing you that the installation was successful.

    Click **Finish**.

13. Start the Access Server so that you can confirm the Access Server is installed and operating properly.

    To start the Access Server, follow these steps:

    a. Go to the following directory:

       ORACLE_HOME/access/oblix/apps/common/bin

       where *ORACLE_HOME* is the location where Oracle Access Manager Access Server is installed.

    b. Execute the following script:

       ```
       start_access_server
       ```

       If you want to use the NPTL threading model, execute the following script instead:

       ```
       start_access_server_nptl
       ```

14. Repeat the preceding steps on OAMHOST2, substituting the hostname where appropriate.

7.4.3 Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2

The third step in installing the Access System is to install WebGate.

This section includes these topics:

- Section 7.4.3.1, "Creating a WebGate Profile"
- Section 7.4.3.2, "Assigning an Access Server to the WebGate"
- Section 7.4.3.3, "Installing the WebGate"

7.4.3.1 Creating a WebGate Profile

The WebGate profile can be created manually or automatically:

- Manual Creation: The WebGate profiles can be created manually by using the Access System Console. If you choose to create the WebGate profiles manually, follow the steps in this section. However, make sure to use appropriate values for the WebGate profile ID and the Host Identifier. These values are passed as parameters to the OAM Configuration Tool to enable single sign-on as discussed in Chapter 8, "Configuring Single Sign-On for Administration Consoles."
- Automatic Creation: The WebGate profiles can be created automatically by the Oracle Access Manager Configuration Tool as discussed in Chapter 8. If you choose to create the WebGate profiles automatically, do the following:
  a. Do not perform the steps in the "Steps for Manually Creating the WebGate Profile Using the Access System Console" section below.
  b. Proceed to Section 8.2, "Running the Oracle Access Manager Configuration Tool" and perform the steps described in that section.
  c. After running the Oracle Access Manager Configuration Tool successfully, return to Section 7.4.3.2, "Assigning an Access Server to the WebGate" and preform the steps in that section.
  d. Perform the steps in Section 7.4.3.3, "Installing the WebGate," using the WebGate profile ID that was created by the OAM Configuration Tool.

Steps for Manually Creating the WebGate Profile using the Access System Console

Follow these steps to create a WebGate profile using the Access System Console:

1. Navigate to the Access System Console by specifying the following URL in your web browser:

   `http://`*`hostname:port`*`/access/oblix`

   where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. On the Access System main page, click the **Access System Console** link, then log in as an Administrator.
3. On the Access System Console main page:

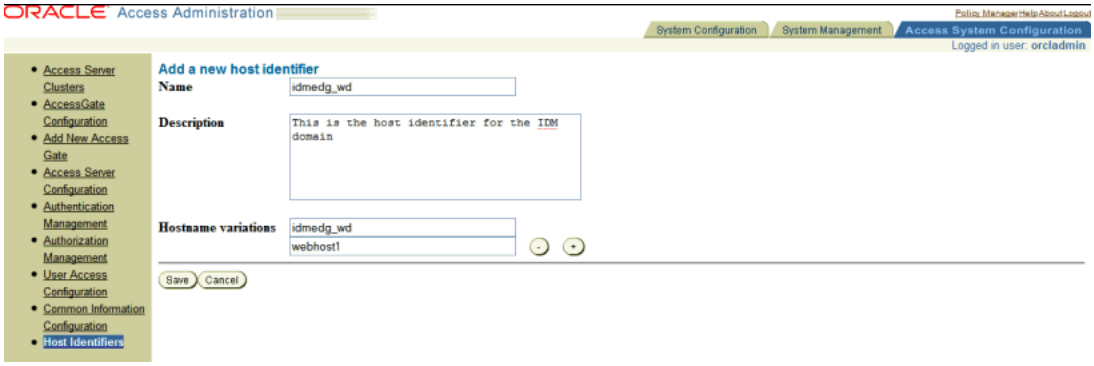
   Click the **Access System Configuration** tab, then select **Host Identifiers**.

   Click **Add**.
4. Specify the following parameters for your host identifier:
   - **Name**: Name of the host identifier. For example: `idmedg_wd`

- **Description**: A brief description of the host identifier. For example: `This is the host identifier for the IDM domain`.
- **Hostname variations**: All possible hostname variations for this host. Click the plus and minus symbols to add or delete fields as necessary. The **Preferred HTTP Host** value used in the Access System Configuration must be added as one of the hostname variations. For example: `idmedg_wd`, `webhost1.mycompany.com:7777, admin.mycompany.com`

Note: One of the hostname variations provided here will be passed as a value for the `web_domain` parameter while running the OAM Configuration Tool to enable Single Sign-On. For more information, refer to Section 8.2.2, "Running the OAM Configuration Tool."

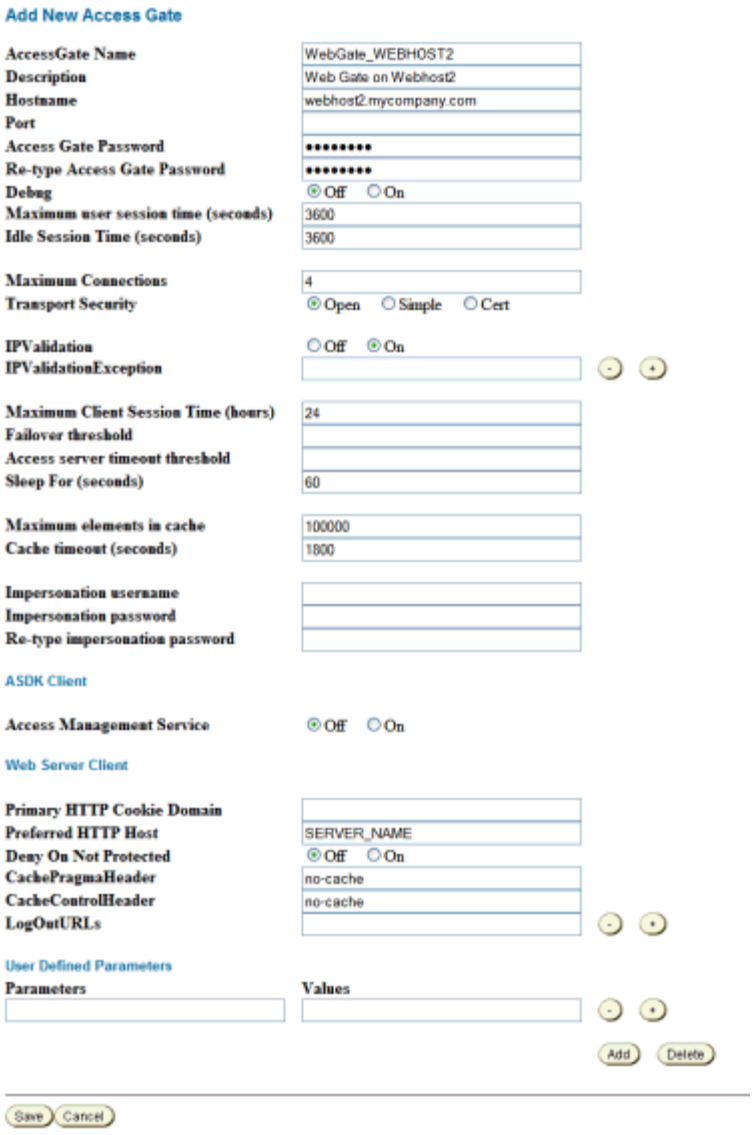
For more information about host identifiers, refer to the *Oracle Access Manager Access Administration Guide*.



5. Click **Access System Configuration**, then select **Add New Access Gate**.
6. Specify the following parameters for your WebGate:
   - **AccessGate Name**: Provide a unique, descriptive name for this WebGate. This is also the WebGate ID or Access Gate ID. For example: `WebGate_WebHost1`
   - **Description**: Specify additional descriptive information about the WebGate. This is an optional parameter.
   - **Hostname**: Specify the name of the computer where the WebGate will be installed. For example: `webhost1.mycompany.com`
   - **Port**: Specify the port the WebGate Web server is listening to. This is an optional parameter.
   - **AccessGate Password and Re-type AccessGate Password**: Enter a password for the WebGate.
   - **Transport Security**: The level of transport security between the Access Server and associated WebGates. Specify **Open** (the transport security mode must be the same between all Access Servers and WebGates).
   - **Maximum Connections**: This parameter is based on how many Access Server connections are defined to each individual Access Server. In this case, the value to be used is 4 (2 connections per access server and there are 2 access servers)

- **Preferred HTTP Host**: The value provided for the Preferred HTTP Host must be one of the following:
  - An existing host identifier as provided in step 4 of this section. For example: `idmedg_wd`
  - SERVER_NAME
  - HOST_HTTP_SERVER

Click **Save**.



7. Details for the WebGate instance appear, and you are prompted to associate an Access Server or Access Server cluster with the WebGate.

   Note the details on this page for future reference, then click the **Back** button.

7.4.3.2 Assigning an Access Server to the WebGate

Follow these steps to assign an Access Server to the WebGate:

1. Log in as the Administrator.
2. Navigate to the **Details for AccessGate** page, if necessary. (From the **Access System Console**, select **Access System Configuration**, then **AccessGate Configuration**, then the link for the WebGate.).
3. On the **Details for AccessGate** page, click **List Access Servers**.
4. A page appears with a message that there are no primary or secondary Access Servers currently configured for this WebGate.

   Click **Add**.
5. On the **Add a new Access Server** page, select an Access Server from the **Select Server** list, specify **Primary Server**, and define **2** connections for the WebGate.

   Click the **Add** button to complete the association.
6. A page appears, showing the association of the Access Server with the WebGate.

   Click the link to display a summary and print this page for use later.
7. Repeat steps 3 through 6 to associate another Access Server to the WebGate.

7.4.3.3 Installing the WebGate

Follow these steps to install the WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2:

1. Locate the WebGate Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console.

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate -gui
   ```
2. On the Welcome to the InstallShield Wizard for Oracle Access Manager WebGate screen, click **Next**.
3. On the Customer Information screen, enter the username and group that the Identity Server will use. The default value for username and group is `nobody`. For example, enter `oracle/oinstall`.

   Click **Next**.
4. Specify the installation directory for Oracle Access Manager Access Server. For example, enter:

   ```
   /u01/app/oracle/product/fmw/oam/webgate
   ```

   Click **Next**.

Note: The base location for the Oracle Access Manager WebGate installation is `/u01/app/oracle/product/fmw/oam/webgate`. The WebGate component is installed in a subdirectory automatically created by the installer under this location.

The WebGate is installed in the `access` subdirectory created by the installer under the base location.

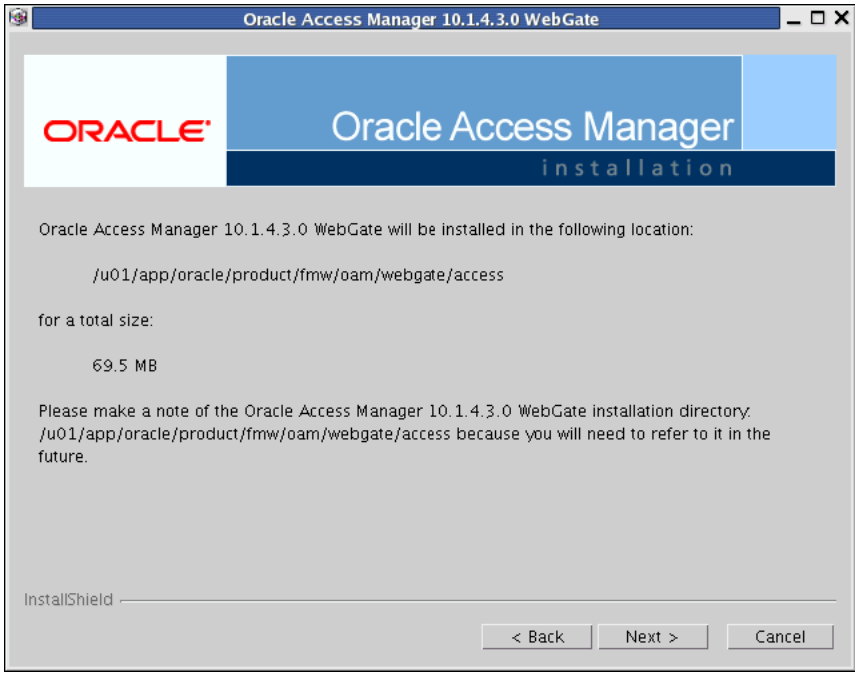
The ORACLE_HOME location for the Oracle Access Manager WebGate installation is:

```
/u01/app/oracle/product/fmw/oam/webgate/access
```

---

5. Oracle Access Manager WebGate will be installed in the following location (the `access` directory is created by the installer automatically):

   `/u01/app/oracle/product/fmw/oam/webgate/access`



6. Specify the location of the GCC runtime libraries, for example: `/home/oracle/oam_lib`.

   Click **Next**.

7. The installation progress screen is shown. After the installation process completes, the WebGate Configuration screen appears.

8. On the WebGate Configuration screen you are prompted for the transport security mode.

   Specify the transport security mode. The transport security between all Access System components (Policy Manager, Access Servers, and associated WebGates) must match; select one of the following: **Open Mode**, **Simple Mode**, or **Cert Mode**.

   Select **Open Mode**.

   Click **Next**.

9. On the next WebGate Configuration screen, specify the following WebGate details:

   - **WebGate ID**: Specify the unique ID that identifies the WebGate profile in the Access System Console. If the profile was created manually, use the Access Gate Name provided in Section 7.4.3.1, "Creating a WebGate Profile." If the profile was created by the OAM Configuration Tool, use the Access Gate ID that is shown in the output after the tool completes successfully. Refer to Section 8.2.2, "Running the OAM Configuration Tool" for more information.
   - **Password for WebGate**: Specify the password defined in the Access System Console.

- **Access Server ID**: Specify the Access Server associated with the WebGate. For example: `AccessServer_OAMHOST1`
- **DNS Hostname**: Specify the DNS host name where the Access Server associated with this WebGate is installed. For example: `oamhost1.mycompany.com`
- **Port Number**: Specify the listen port for the Access Server.

Click **Next**.

10. On the Configure Web Server screen, click **Yes** to automatically update the web server, then click **Next**.
11. On the next Configure Web Server screen, specify the full path of the directory containing the `httpd.conf` file. The httpd.conf file is located under the following directory:

    `/u01/app/oracle/admin/`*`ohsInstance`*`/config/OHS/`*`ohsComponentName`*

    For example:

    `/u01/app/oracle/admin/ohs_instance2/config/OHS/ohs2/httpd.conf`

    Click **Next**.
12. On the next Configure Web Server page, a message informs you that the Web Server configuration has been modified for WebGate.

    Click **Next**.
13. Stop and start your Web server to enable configuration updates to take effect.

    Click **Next**.

14. On the next Configure Web Server screen, the following message is displayed: "If the web server is setup in SSL mode, then httpd.conf file needs to be configured with the SSL related parameters. To manually tune your SSL configuration, please follow the instructions that come up".

    Click **Next**.

15. On the next Configure Web Server screen, a message with the location of the document that has information on the rest of the product setup and Web Server configuration is displayed.

    Select **No** and click **Next**.

16. The final Configure Web Server screen appears with a message to manually launch a browser and open the html document for further information on configuring your Web Server.

    Click **Next**.

17. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next**.

18. A message appears (along with the details of the installation) informing you that the installation was successful.

    Click **Finish**.

19. Restart your Web server.

20. Verify the installation by performing the following steps:

    a. Ensure that the Identity Server, WebPass Web server, Policy Manager and Web Server, Access Server, and WebGate Web Server are running.

    b. Specify the following URL for WebGate diagnostics:

    ```
    http(s)://hostname:port/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
    ```

    Where *hostname* refers to the host where the WebGate instance is running and *port* refers to HTTP port of the Oracle HTTP Server instance that is associated with the WebGate instance.

    For example, use these URLs for the WebGate on each of the following hosts:

    ```
    OAMADMINHOST:
    http(s)://oamadminhost.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1

    WEBHOST1:
    http(s)://webhost1.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1

    WEBHOST2:
    http(s)://webhost2.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
    ```

    The WebGate diagnostic page should appear. If the WebGate diagnostic page appears, the WebGate is functioning properly and you can dismiss the page.

7.5 Backing Up the Oracle Access Manager Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a

quick backup for the express purpose of immediate restore in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

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

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

1. Back up the Oracle Access Manager Identity Server.
   a. Stop the Identity Server using the `stop_ois_server` script located under the *`Identity_Server_ORACLE_HOME`*`/oblix/apps/common/bin` directory.
   b. Create a backup of the *`Identity_Server_ORACLE_HOME`* directory as the `root` user:

      ```
      tar -cvpf BACKUP_LOCATION/IdentityServer.tar Identity_Server_ORACLE_HOME
      ```

   c. Start the Identity Server using the `start_ois_server` script located under the *`Identity_Server_ORACLE_HOME`*`/oblix/apps/common/bin` directory.
2. Back up the Oracle Access Manager Access Server.
   a. Stop the Access Server using the `stop_access_server` script located under the *`Access_Server_ORACLE_HOME`*`/oblix/apps/common/bin` directory.
   b. Create a backup of the *`Access_Server_ORACLE_HOME`* directory as the `root` user:

      ```
      tar -cvpf BACKUP_LOCATION/accessServer.tar Access_Server_ORACLE_HOME
      ```

   c. Start the Access Server using the `start_access_server` script located under the *`Access_Server_ORACLE_HOME`*`/oblix/apps/common/bin` directory.
3. Back up the Oracle Access Manager WebPass, Policy Manager, Oracle HTTP Server, and WebGate.
   a. Stop the Oracle Access Manager WebPass, Policy Manager, Webgate and Oracle HTTP Server instance. Stopping the Oracle HTTP Server instance using `opmnctl` stops all four components, for example:

      ```
      ORACLE_INSTANCE/bin/opmnctl stopall
      ```

   b. Create a backup of the Oracle HTTP Server Middleware Home on the web tier as the `root` user:

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

   c. Create a backup of the INSTANCE_HOME on the web tier as the `root` user:

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

   d. Create a backup of the WebPass and Policy Manager ORACLE_HOMEs as the `root` user:

      ```
      tar -cvpf BACKUP_LOCATION/webPass.tar WEBPASS_ORACLE_HOME
      tar -cvpf BACKUP_LOCATION/policyMgr.tar POLICY_MGR_ORACLE_HOME
      ```

e. Create a backup of the WebGate ORACLE_HOME as the `root` user:

```
tar -cvpf BACKUP_LOCATION/webGate.tar WEBGATE_ORACLE_HOME
```

f. Start up the instance using `opmnctl` under the *ORACLE_INSTANCE*`/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

4. Back up the directory tier:

a. Shut down the instance using `opmnctl` located under the *ORACLE_INSTANCE*`/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

b. Create a backup of the Middleware Home on the directory tier as the `root` user:

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

c. Create a backup of the INSTANCE_HOME on the directory tier as the `root` user:

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

d. Start up the instance using `opmnctl` under the *ORACLE_INSTANCE*`/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

Note: Create backups on all the machines in the directory tier by following the steps shown above.

---

5. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. An operating system tool such as `tar` can be used for cold backups.

6. Back up the Administration Server domain directory. This saves your domain configuration. All the configuration files exist under the *MW_HOME*`/user_projects/domains/`*domainName* directory:

```
IDMHOST1> tar cvf edgdomainback.tar MW_HOME/user_projects/domains/domainName
```

For more information about backing up the Oracle Access Manager configuration, see Section 10.4, "Performing Backups and Recoveries."

8

Configuring Single Sign-On for Administration Consoles

This chapter describes how to configure single sign-on for administration consoles. The administration consoles referred to in the chapter title are:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console

This chapter includes the following topics:

8.1 Prerequisites for Configuring Single Sign-On

Make sure that these steps have been performed before moving on to the next section:

1. Oracle Access Manager has been installed and configured as described in Chapter 7, "Installing and Configuring Oracle Access Manager."
2. Ensure that the policy protecting the Policy Manager ("/access") has been created and enabled. If this is not enabled, use the Policy Manager console to enable it. Follow the steps below to enable this policy:
   a. Open a web browser and bring up the Policy Manager Console using the following URL:

      ```
      http://oamadminhost.mycompany.com:7777/access/oblix
      ```

   b. Click the **Policy Manager** link.
   c. On the Policy Manager landing page, click the **My Policy Domains** link.
   d. On the My Policy Domains page, click the **Policy Manager** link.
   e. On the **General** tab on the Policy Manager page, click **Modify**.

f. Click **Yes** to enable the "/access" policy.

g. Click the **Save** button to save the changes.

3. If a WebGate profile was set up manually by following the steps in Section 7.4.3.1, "Creating a WebGate Profile" or if you are planning on using an existing WebGate, make sure that the host identifier has been set up properly. The host identifier value is required for enabling single sign-on.

8.2 Running the Oracle Access Manager Configuration Tool

The Oracle Access Manager Configuration tool (OAM Configuration tool) is a command line utility provided to automatically enable single sign-on with Oracle Access Manager. The OAM Configuration tool runs a series of scripts and sets up the required policies. It requires a set of parameters as inputs. Specifically, the tool creates the following:

- A Form Authentication scheme in Oracle Access Manager
- Policies to enable authentication in the Oracle WebLogic Server
- Optionally, a WebGate profile in Oracle Access Manager to enable Oracle HTTP Server WebGates (from your web tier) to protect your configured applications. When this option is selected a WebGate profile is created for every application configured using the tool.
- A host identifier, depending on the scenario you choose. The host identifier is used to configure the WebGate hosts that send requests to your application. When a host identifier is not supplied, a default one is created with the "app_domain" name.
- Policies to protect and un-protect application-specific URLs. These policies would be configured for the host identifier created or provided in the previous step.

Note: If you plan on using an existing WebGate, the host identifier value of this WebGate must be used for the `web_domain` parameter when running the OAM Configuration tool.

8.2.1 Collecting the Information for the OAM Configuration Tool

Before you run the OAM Configuration tool, collect the following information:

- LDAP Host: The host name of the Directory Server or a load balancer address (in the case of a high availability or enterprise deployment configuration).
- LDAP Port: The port of the Directory Server.
- LDAP USER DN: The DN of the LDAP Administrator user. This will be a value such as `cn=orcladmin`.
- LDAP Password: Password of the LDAP Administrator user.
- oam_aaa_host: The host name of an Oracle Access Manager.
- oam_aaa_port: The port of an Oracle Access Manager.

8.2.2 Running the OAM Configuration Tool

The OAM Configuration tool is located in the directory shown below. This tool can be run from any host that has Oracle Fusion Middleware 11*g* Release 1 installed.

ORACLE_HOME/modules/oracle.oamprovider_11.1.1/

Set the JAVA_HOME value before running the tool as shown below:

```
export JAVA_HOME=$MW_HOME/jrockit_160_05_R27.6.2-20
```

The syntax for using the OAM Configuration tool is:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE [param=value]...
```

Table 8–1 shows the basic OAM Configuration tool parameters and their values.

Table 8–1 Basic Parameters for the OAM Configuration Tool

Parameter	Value
app_domain	Oracle Access Manager policy domain name
web_domain	Name of the web domain. If you choose the tool to automatically created a WebGate profile entry, do not pass this parameter. If you manually created a WebGate profile, use the value of the host identifier for that WebGate. Refer to Section 7.4.3.1, "Creating a WebGate Profile" for more information.
protected_uris	"uri1,uri2,uri3"
app_agent_password	Password to be provisioned for App Agent
ldap_host	Host name of LDAP server
ldap_port	Port of LDAP server
ldap_userdn	DN of LDAP Administrator user
ldap_userpassword	Password of LDAP Administrator user
oam_aaa_host	Host name of an Oracle Access Manager
oam_aaa_port	Port of an Oracle Access Manager

The OAM Configuration tool has optional parameters that can be used for CREATE mode. Table 8–2 shows those parameters.

Table 8–2 OAM Configuration Tool Optional Parameters for CREATE Mode

Parameter	Value
cookie_domain	Domain name to use for Single Sign-On cookie
public_uris	"uri1,uri2,uri3"
ldap_base	Base DN from which all LDAP searches will be done
oam_aaa_mode	One of OPEN, SIMPLE, CERT. Defaults to OPEN.
oam_aaa_passphrase	Passphrase required for SIMPLE mode
log_file	Name of the log file. Defaults to console output
log_level	One of ALL, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, OFF. Defaults to OFF.
output_ldif_file	Name of the LDIF file to store changes. If specified, will generate LDIF to be loaded later.

This is an example command for running the OAM Configuration tool when you want the tool to create a WebGate profile:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE app_domain="IDMEDG"
```

```
cookie_domain=".mycompany.com"
protected_uris="/em,/console" app_agent_password="welcome1"
ldap_host=oid.us.oracle.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=password oam_aaa_host=oamhost1.mycompany.com
oam_aaa_port=6023
```

Note: The `web_domain` parameter should not be provided when you use the OAM Configuration Tool to create the WebGate profile.

The following output is displayed when the command completes successfully:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
 Operation Summary:
     Policy Domain  : IDMEDG
     Host Identifier: IDMEDG
     Access Gate ID : IDMEDG_AG
```

Note: The Access Gate ID value above should be used as the WebGate ID when performing the WebGate installation described in Section 7.4.3.3, "Installing the WebGate."

This is an example command for running the OAM Configuration tool when you plan on using an existing WebGate:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE app_domain="IDMEDG"
web_domain="idmEDG_WD" cookie_domain=".mycompany.com"
protected_uris="/em,/console" app_agent_password="welcome1"
ldap_host=oid.us.oracle.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=<password> oam_aaa_host=oamhost1.mycompany.com
oam_aaa_port=6023
```

The following output is displayed when the command completes successfully:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
 Operation Summary:
     Policy Domain  : IDMEDG
     Host Identifier: idmedg_wd
     Access Gate ID : idmedg_wd_AG
```

To validate that the tool created the policies correctly, run the tool in VALIDATE mode:

```
java -jar oamcfgtool.jar mode=VALIDATE app_domain="IDMEDG"
ldap_host=oid.mycompany.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=welcome1 oam_aaa_host=oamhost1.mycompany.com oam_aaa_port=6023
test_username=orcladmin test_userpassword=welcome1
```

The output from the VALIDATE command is shown below:

```
Processed input parameters
Initialized Global Configuration
Validating app_domain: IDMEDG : OK.
```

```
Validating web_domain: IDMEDG : OK.
Validating access_gate: IDMEDG_AG : OK.
Found url:http://IDMEDG/public
Found url:http://IDMEDG/em
Found url:http://IDMEDG/console
Successfully completed the Validate operation
```

8.2.3 Update the Host Identifier

The OAM Configuration Tool uses the value of the `app_domain` parameter to create a host identifier for the policy domain. This host identifier must be updated with all the hostnames variations for the host so that the configuration works correctly. Follow the steps below to update the host identifier created by the OAM Configuration Tool:

1. Navigate to the Access System Console by specifying the following URL in your web browser:

   `http://`*`hostname`*`:`*`port`*`/access/oblix`

   where *`hostname`* refers to the host where WebPass Oracle HTTP Server instance is running and *`port`* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. When prompted for a username and password, log in as an Administrator. Click **OK**.
3. On the Access System main page, click the **Access System Console** link.
4. On the Access System Console page, click the Access System Configuration tab.
5. On the Access System Configuration page, click **Host Identifiers** at the bottom left.
6. On the List all host identifiers page, click on the host identifier created by the OAM Configuration Tool. For example, select `IDMEDG`.
7. On the Host Identifier Details page, click **Modify**.
8. On the Modifying host identifier page, add all the possible hostname variations for the host. Click the plus and minus symbols to add or delete fields as necessary. The **Preferred HTTP Host** value used in the Access System Configuration must be added as one of the hostname variations. For example: `idmedg_wd`, `webhost1.mycompany.com:7777`, `admin.mycompany.com:7777`
9. Select the check box next to Update Cache and then click **Save**.

   A message box with the following message is displayed: "Updating the cache at this point will flush all the caches in the system. Are you sure?"

   Click **OK** to finish saving the configuration changes.
10. Verify the changes on the Host Identifier Details page.

8.2.4 Update the WebGate Profile

The OAM Configuration Tool populates the `Preferred_HTTP_Host` and `hostname` attributes for the WebGate profile that is created with the value of the `app_domain` parameter. Both these attributes must be updated with the proper values for the

configuration to work correctly. Follow the steps below to update the WebGate profile created by the OAM CFG Tool.

1. Navigate to the Access System Console by specifying the following URL in your web browser:

   `http://hostname:port/access/oblix`

   where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. On the Access System main page, click the **Access System Console** link, then log in as an Administrator.
3. On the Access System Console main page, click the **Access System Configuration** link to display the AccessGates Search page.
4. Enter the proper search criteria and click **Go** to display a list of AccessGates.
5. Select the AccessGate created by the OAM Configuration Tool. For example: `IDMEDG_AG`
6. On the AccessGate Details page, select **Modify** to display the Modify AccessGate page.
7. On the Modify AccessGate page, update:
   - **Hostname**: Update the hostname with the name of the computer where WebGate is running. For example: `webhost1.mycompany.com`
   - **Preferred HTTP Host**: Update the Preferred_HTTP_Host with one of the hostname variations specified in the previous section, for example: `admin.mycompany.com:7777`
8. Click **Save**. A message box with the "Are you sure you want to commit these changes?" message is displayed.
9. Click **OK** to finish updating the configuration.
10. Verify the values displayed on the Details for AccessGate page to confirm that the updates were successful.

8.2.5 Update the Form Authentication for Delegated Administration

The WebGates in the IDM Domain also need to act as delegated authentication WebGates, that is, they receive authentication requests from external applications or domains in the enterprise. To enable delegated authentication, the form authentication scheme created by the OAM Configuration Tool must be modified to add the Challenge Redirect parameter.

Follow the steps below to add the challenge redirect parameter to the Form authentication scheme:

1. Use a web browser to display the Access Console using the URL below:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. Click the Access System Console link and log in using the credentials for the `orcladmin` user.
3. On the main page, click the Access System Configuration tab.

4. On the Access System Configuration page, click the **Authentication Management** link on the left hand side.
5. On the Authentication Management page, under the **List all Authentication Schemes** table, click the link for form authentication scheme created by the tool. The form authentication scheme created by the tool is called `OraDefaultFormAuthNScheme`.
6. On the Details for Authentication Scheme page, click **Modify** to modify the configuration of the authentication scheme.
7. On the Modifying Authentication Scheme page, update the Challenge Redirect parameter with the Single Sign-On virtual host configured in the load balancer. Use `https://sso.mycompany.com` to update the Challenge Redirect parameter.
8. Click **Save** to save the updated configuration.
9. To validate that the configuration was successful, follow the steps below:
   a. Using a web browser, bring up either the Oracle WebLogic Administration Console or Oracle Enterprise Manager Fusion Middleware Control:

      URL for the WebLogic Administration Server Console:

      ```
      http://admin.mycompany.com:7777/console
      ```

      URL for the Enterprise Manager Oracle Fusion Middleware Control:

      ```
      http://admin.mycompany.com:7777/em
      ```

   b. Log into the console using the `administrator` user's credentials.
   c. This will redirect your web browser to `http://sso.mycompany.com` during authentication.

8.3 Validating the Policy Domain and AccessGate Configurations

The next part of the process is to validate the policy domain configuration and the AccessGate configuration.

8.3.1 Validating the Policy Domain Configuration

Follow these steps to verify that the policy domain was created properly:

1. In a web browser, enter this URL to access the Oracle Access Manager console:

   ```
   http://OAMADMINHOST:port/access/oblix
   ```

2. Click **Policy Manager**.
3. Click the **My Policy Domains** link on the left panel. You will see a list of all the policy domains, which includes the domain you just created. For example: `IDMEDG`. In the third column, **URL prefixes**, you will see the URIs you specified when creating the policy domain).
4. Click the link to the policy domain you just created. This displays the General area of this domain.
5. Click the Resources tab. On this tab you can see the URIs you specified. Click other tabs to view other settings.

8.3.2 Validating the AccessGate Configuration

Follow these steps to verify that the AccessGate was configured properly:

1. In the Oracle Access Manager console, click the **Access System Console** link. This link is a toggle. When it is the **Access System Console** link and you click it, it becomes the **Policy Manager** link. When it is the **Policy Manager** link and you click it, it becomes the **Access System Console** link.
2. Click the **Access System Configuration** tab.
3. Click the **AccessGate Configuration** link on the left panel.
4. Enter some search criteria and click **Go**.
5. When the name of the AccessGate for the domain you created appears (it may have the suffix _AG when created by the OAM Configuration Tool, for example, IDMEDG_AG), click it to view the details of the AccessGate you created.

8.4 Setting Up the WebLogic Authenticators

This section describes the steps for setting up Oracle WebLogic Server authenticators.

8.4.1 Setting Up the Oracle Internet Directory Authenticator

Follow these steps to set up the Oracle Internet Directory authenticator:

1. Begin by backing up these relevant configuration files:

   DOMAIN_HOME/config/config.xml

   DOMAIN_HOME/config/fmwconfig/jps-config.xml

   DOMAIN_HOME/config/fmwconfig/system-jazn-data.xml

2. Back up the *DOMAIN_HOME*/servers/adminServer/boot.properties file for the Administrator Server.
3. Follow these steps to configure the Identity Store to use LDAP, setting the proper authenticator using the WebLogic Administration Server Console:
   a. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
   b. Click the **Security Realms** link on the left navigational bar.
   c. Click the **myrealm** default realm entry to configure it.
   d. Click the **Providers** tab within the realm.
   e. Note that there is a DefaultAuthenticator provider configured for the realm.
   f. Click the **New** button to add a new provider.
   g. Enter a name for the provider, such as "OIDAuthenticator" for a provider that will authenticate the user to the Oracle Internet Directory.
   h. Select the "OracleInternetDirectoryAuthenticator" type from the list of authenticators.
   i. Click **OK**.
   j. On the Providers screen, click the newly created OIDAuthenticator.

k. Set the Control Flag to **SUFFICIENT**. This indicates that if a user can be authenticated successfully by this authenticator, then it is should accept that authentication and should not continue to invoke any additional authenticators. If the authentication fails, it will fall through to the next authenticator in the chain. Make sure all subsequent authenticators also have their control flag set to **SUFFICIENT** also. In particular, check the DefaultAuthenticator and set that to **SUFFICIENT**.

l. Click **Save** to save this setting.

m. Click the **Provider Specific** tab to enter the details for the LDAP server.

n. Enter the details specific to your LDAP server, as shown in the following table:

Parameter	Value	Description
Host		The LDAP server's server ID. For example: `oid.mycompany.com`
Port		The LDAP server's port number. For example: `636`
Principal		The LDAP user DN used to connect to the LDAP server. For example: `cn=orcladmin`
Credential		The password used to connect to the LDAP server
SSL Enabled	Checked	Specifies whether SSL protocol is used when connecting to LDAP server.
User Base DN		Specify the DN under which your Users start. For example: `cn=users,dc=us,dc=mycompany,dc=com`
Group Base DN		Specify the DN that points to your Groups node. For example: `cn=groups,dc=us,dc=mycompany,dc=com`
Use Retrieved User Name as Principal	Checked	Must be turned on.

Click **Save** when done.

o. Click **Activate Changes** to propagate the changes.

p. The console displays a message that a restart is required for the changes to take effect. Do not restart the servers as indicated; this will be done after setting up all the WebLogic Authenticators, as described in Section 8.4.4, "Stop and Start the WebLogic Administration Servers and Managed Servers."

8.4.2 Setting Up the OAM ID Asserter

Follow these steps to set up the OAM ID Asserter:

1. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
2. Navigate to **SecurityRealms** > *Default Realm Name* > **Providers**.
3. Click **New** and select **OAM Identity Asserter** from the drop down menu.
4. Name the asserter, for example: `OAM ID Asserter`

   Then click **OK**.

5. Click the newly-added asserter to see the configuration screen for OAM Identity Asserter.
6. Set the Control Flag to **REQUIRED**, and then click **Save**.
7. Configure the additional attributes below for the OAM Identity Asserter on the **Provider Specific** tab:
   - **Application Domain**: Provide the Oracle Access Manager policy domain name. Use the `app_domain` parameter passed to the OAM Configuration Tool. For example: `IDMEDG`.
   - **Primary Access Server**: Provide Oracle Access Manager server endpoint information in the *host*:*port* format. For example: `oamhost1.mycompany.com: 6023`
   - **Application Domain**: Provide the Oracle Access Manager policy domain name. Use the `app_domain` parameter passed to the OAM Configuration Tool. For example: `IDMEDG`.
   - **AccessGate Name**: Name of the AccessGate (for example, IDMEDG_WD). Use the AccessGate name created by the OAM Configuration Tool or created manually in Section 7.4.3.1, "Creating a WebGate Profile."
   - **AccessGate Password**: Password for the AccessGate, if one was provided.

   Accept the default values for all the other attributes, unless required for your environment.
8. Save the settings.
9. Click **Activate Changes** to propagate the changes.

8.4.3 Reorder OAM Identity Asserter, OID Authenticator, and Default Authenticator

Follow the steps below to reorder the providers in the order shown below:

1. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
2. Navigate to **SecurityRealms >** *Default Realm Name* **> Providers**.
3. Ensure that the Control Flag for each authenticator is set correctly.
4. Click **Reorder** under the **Authentication Providers** table.
5. On the Reorder Authentication Providers page, reorder the providers as shown below:

```
OAM Identity Asserter (REQUIRED) > OID Authenticator (SUFFICIENT) >
Default Authenticator (SUFFICIENT) > DefaultIdentityAsserter
```

6. Save the settings.
7. Click **Activate Changes** to propagate the changes.

8.4.4 Stop and Start the WebLogic Administration Servers and Managed Servers

The WebLogic Administration Server and the associated Managed Servers must be restarted for the configuration changes to take effect. Follow the steps below to stop and then start the WebLogic Administration Server and the Managed Servers (`wls_ods1` and `wls_ods2`):

1. Using the WebLogic Administration Server Console, stop the Administration Server and the `wls_ods1` and `wls_ods2` Managed Servers.

2. Verify that the server processes have been successfully stopped.
3. On IDMHOST1, start the WebLogic Administration Server using the `startWebLogic.sh` script located under the *DOMAIN_HOME*`/bin` directory using the syntax below. This enables the standard output log messages shown on the screen to be written to the file specified in the `logfile` parameter.

   ```
   ./startWebLogic.sh >logfile 2>&1 &
   ```

   For example:

   ```
   ./startWebLogic.sh >$DOMAIN_HOME/servers/AdminServer/logs/aserver.out 2>&1 &
   ```

4. Verify that the Administration Server has started up and then bring up the Administration Console using a web browser.
5. Log into the console using the `administrator` user's credentials.
6. Start the `wls_ods1` and `wls_ods2` Managed Servers using the WebLogic Administration Console.

8.5 Changing the Login Form for the Administration Server

To enable the Oracle WebLogic Administration Server Console application to direct login requests to its root, update the `web.xml` file by following these steps:

1. Make a backup copy of the following file:

   ORACLE_BASE`/fmw/wlserver_10.3/server/lib/consoleapp/webapp/WEB-INF/web.xml`

   For example:

   ```
   cp ORACLE_BASE/fmw/wlserver_10.3/server/lib/consoleapp/webapp/WEB-INF/web.xml
   ORACLE_BASE/fmw/wlserver_10.3/server/lib/consoleapp/webapp/WEB-INF/
   web.xml.backup
   ```

2. Edit the `web.xml` file and change the `form-login-page` URL to "/".

   Specifically, change:

   ```
   login-config>
       <auth-method>CLIENT-CERT,FORM</auth-method>
       <form-login-config>
         <form-login-page>/login/LoginForm.jsp</form-login-page>
         <form-error-page>/login/LoginError.jsp</form-error-page>
       </form-login-config>
     </login-config>
   ```

   to:

   ```
   <login-config>
       <auth-method>CLIENT-CERT,FORM</auth-method>
       <form-login-config>
         <form-login-page>/</form-login-page>
         <form-error-page>/login/LoginError.jsp</form-error-page>
       </form-login-config>
     </login-config>
   ```

3. Restart the Administration Server.
4. Validate that the changes made were successful by bringing up the Administration Server Console.

8.6 Creating WebLogic Administrative Users in an LDAP Directory

In an enterprise, it is typical to have a centralized Identity Management domain where all users, groups and roles are provisioned and multiple application domains (such as a SOA domain and WebCenter domain). The application domains are configured to authenticate using the central Identity Management domain.

By default, when the Oracle WebLogic Server is installed and configured, the WebLogic admin user is created in its local LDAP store with the username `weblogic`. For an enterprise deployment, it is required to have all users, groups provisioned in an LDAP user directory such as Oracle Internet Directory that is a part of the centralized Identity Management Domain. This section provides details for provisioning a new administrator user and group for managing the Identity Management WebLogic Domain. This section describes the following:

- Section 8.6.1, "Provisioning Admin Users and Groups in an LDAP Directory"
- Section 8.6.2, "Assigning the Admin Role to the Admin Group"
- Section 8.6.3, "Updating the boot.properties File on IDMHOST1 and IDMHOST2"

8.6.1 Provisioning Admin Users and Groups in an LDAP Directory

As mentioned in the introduction to this section, users and groups from multiple WebLogic domains may be provisioned in a central LDAP user store. In such a case, there is a possibility that one WebLogic `admin` user may have access to all the domains within an enterprise. This is not a desirable situation. To avoid this, the users and groups provisioned must have a unique distinguished name within the directory tree. In this guide, the `admin` user and group for the IDM WebLogic Domain will be provisioned with the DNs below:

- Admin User DN:

  cn=weblogic_idm,cn=Users,dc=us,dc=mycompany,dc=com

- Admin Group DN:

  cn=IDM Administrators, cn=Groups,dc=us,dc=mycompany,dc=com

Follow the steps below to provision the `admin` user and `admin` group in Oracle Internet Directory:

1. Create an `ldif` file named `admin_user.ldif` with the contents shown below and then save the file:

```
dn: cn=weblogic_idm, cn=Users, dc=us, dc=mycompany, dc=com
orclsamaccountname: weblogic_idm
givenname: weblogic_idm
sn: weblogic_idm
userpassword: Welcome1
obver: 10.1.4.0
mail: weblogic_idm
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
objectclass: oblixorgperson
uid: weblogic_idm
cn: weblogic_idm
description: Admin User for the IDM Domain
```

2. Run the `ldapadd` command located under the *ORACLE_HOME*`/bin/` directory to provision the user in Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f admin_user.ldif
```

3. Create an `ldif` file named `admin_group.ldif` with the contents shown below and then save the file:

```
dn: cn=IDM Administrators, cn=Groups, dc=us, dc=mycompany, dc=com
displayname: IDM Administrators
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_idm,cn=users,dc=us,dc=mycompany,dc=com
cn: IDM Administrators
description: Administrators Group for the IDM Domain in OID
```

4. Run the `ldapadd` command located under the *ORACLE_HOME*`/bin/` directory to provision the group in Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f admin_group.ldif
```

8.6.2 Assigning the Admin Role to the Admin Group

After adding the users and groups to Oracle Internet Directory, the group must be assigned the Admin role within the WebLogic domain security realm. This enables all users that belong to the group to be administrators for that domain. Follow the steps below to assign the Admin role to the Admin group:

1. Log into the WebLogic Administration Server Console.
2. In the left pane of the console, click **Security Realms**.
3. On the Summary of Security Realms page, click **myrealm** under the **Realms** table.
4. On the Settings page for `myrealm`, click the **Roles & Policies** tab.
5. On the Realm Roles page, expand the **Global Roles** entry under the **Roles** table. This brings up the entry for Roles. Click on the **Roles** link to bring up the Global Roles page.
6. On the Global Roles page, click the **Admin Role** to bring up the Edit Global Role page:
   a. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.
   b. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.
   c. On the Edit Arguments Page, Specify **IDM Administrators** in the **Group Argument** field and click **Add**.
7. Click **Finish** to return to the Edit Global Rule page.
8. The **Role Conditions** table now shows the `IDM Administrators Group` as an entry.
9. Click **Save** to finish adding the Admin Role to the `IDM Administrators Group`.

10. Validate that the changes were successful by bringing up the WebLogic Administration Server Console using a web browser. Log in using the credentials for the `weblogic_idm` user.

8.6.3 Updating the boot.properties File on IDMHOST1 and IDMHOST2

The `boot.properties` file for the Administration Server and the Managed Servers should be updated with the WebLogic `admin` user created in Oracle Internet Directory. Follow the steps below to update the `boot.properties` file.

For the Administration Server on IDMHOST1

1. On IDMHOST1, go the following directory:

   `MW_HOME/user_projects/domains/`*`domainName`*`/servers/`*`serverName`*`/security`

   For example:

   ```
   cd /u01/app/oracle/product/fmw/user_
   projects/domains/IDMDomain/servers/AdminServer/security
   ```

2. Rename the existing `boot.properties` file.

3. Use a text editor to create a file called boot.properties under the security directory. Enter the following lines in the file:

   ```
   username=adminUser
   password=adminUserPassword
   ```

   For example:

   ```
   username=weblogic_idm
   password=Password for weblogic_idm user
   ```

   Note: When you start the Administration Server, the username and password entries in the file get encrypted.

   For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

Stop and Start the Servers

1. Using the WebLogic Administration Server Console, stop the Administration Server and the `wls_ods1` and `wls_ods2` Managed Servers.

2. Verify that the server processes have been successfully stopped.

3. On IDMHOST1, start the WebLogic Administration Server using the `startWebLogic.sh` script located under the *`DOMAIN_HOME`*`/bin` directory using the syntax below. This enables the standard output log messages shown on the screen to be written to the file specified in the `logfile` parameter:

   `./startWebLogic.sh >`*`logfile`*` 2>&1 &`

   For example:

   ```
   ./startWebLogic.sh >$DOMAIN_HOME/servers/AdminServer/logs/aserver.out 2>&1 &
   ```

4. Verify that the Administration Server has started up and then bring up the Administration Console using a web browser.

5. Log in using the credentials of the `weblogic_idm` user.
6. Start the `wls_ods1` and `wls_ods2` Managed Servers using the WebLogic Administration Console.

8.7 Policy and Credential Store Migration

You begin policy and credential store migration by creating the JPS root and then you reassociate the policy and credential store with Oracle Internet Directory.

8.7.1 JPS Root Creation

Create the jpsroot in Oracle Internet Directory using the command line `ldapadd` command as shown in these steps:

1. Create an `ldif` file similar to this:

```
dn: cn=jpsroot_idm_idmhost1
cn: jpsroot_idm_idmhost1
objectclass: top
objectclass: orclcontainer

dn: cn=jpsroot_idm_idmhost2
cn: jpsroot_idm_idmhost2
objectclass: top
objectclass: orclcontainer
```

2. Use *ORACLE_HOME*`/bin/ldapadd` to add these entries to Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f jps_root.ldif
```

8.7.2 Reassociate the Policy and Credential Store

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST `reassociateSecurityStore` command. Follow these steps:

1. From IDMHOST1, start the `wlst` shell from the *ORACLE_HOME*`/common/bin` directory. For example:

```
./wlst.sh
```

2. Connect to the WebLogic Administration Server using the `wlst connect` command shown below.

```
connect('AdminUser',"AdminUserPassword",t3://hostname:port')
```

For example:

```
connect("weblogic_idm,"welcome1","t3://idmhost-vip.mycompany.com:7001")
```

3. Run the `reassociateSecurityStore` command as shown below:

Syntax:

```
reassociateSecurityStore(domain="domainName",admin="cn=orcladmin",
password="orclPassword",ldapurl="ldap://LDAPHOST:LDAPPORT",servertype="OID",
jpsroot="cn=jpsroot_idm_idmhost1")
```

For example:

```
wls:/IDMDomain/serverConfig> reassociateSecurityStore(domain="IDMDomain",
admin="cn=orcladmin",password="welcome1",
ldapurl="ldap://oid.mycompany.com:389",servertype="OID",
jpsroot="cn=jpsroot_idm_idmhost1")
```

The output for the command is shown below:

```
{servertype=OID, jpsroot=cn=jpsroot_idm_idmhost1, admin=cn=orcladmin,
domain=IDMDomain, ldapurl=ldap://oid.mycompany.com:389, password=welcome1}
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)

Starting Policy Store reassociation.
LDAP server and  ServiceConfigurator setup done.

Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Policy Store reassociation done.
Starting credential Store reassociation
LDAP server and  ServiceConfigurator setup done.
Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Credential Store reassociation done
Jps Configuration has been changed. Please restart the server.
```

4. Restart the Administration Server after the command completes successfully.

8.8 Validate the Oracle Access Manager Single Sign-On Setup

To validate the setup, open a web browser and go the following URLs:

```
http://admin.mycompany.com:7777/console

http://admin.mycompany.com:7777/em
```

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

9

Enabling Administration Server High Availability

The Oracle Weblogic Administration Server is a singleton application, so it cannot be deployed in an active-active configuration. By default, the Administration Server is only available on the first installed node, and for this enterprise topology, it is available only on `idmhost1.mycompany.com`. If this node became unavailable, then the Administration Server console and the Oracle Enterprise Manager Fusion Middleware Control would also be unavailable. This is an undesirable scenario. To avoid this scenario, the Administration Server and the applications deployed to it must be enabled for high availability.

This chapter describes how to enable high availability for the Oracle WebLogic Administration Server on IDMHOST2.

It includes the following topics:

- Section 9.1, "Configuring High Availability for Oracle WebLogic Administration Server"
- Section 9.2, "Provisioning the Administration Server and Fusion Middleware Control on IDMHOST2"
- Section 9.3, "Validating Administration Server and Oracle Fusion Middleware Control Failover on IDMHOST2"

9.1 Configuring High Availability for Oracle WebLogic Administration Server

Oracle WebLogic Administration Server is only deployed on IDMHOST1 and the Oracle WebLogic Server installer does not support deploying the Administration Server in an active-active configuration. To avoid creating a potential single point of failure, the Administration Server must be manually enabled for high availability.

This section describes how to configure high availability for the Oracle WebLogic Administration Server and includes the following sections.

- Section 9.1.1, "Enabling a Virtual IP Address on IDMHOST1"
- Section 9.1.2, "Create a Machine for the Administration Server"
- Section 9.1.3, "Enable the Administration Server to Listen on the Virtual IP Address"
- Section 9.1.4, "Update Enterprise Manager Agent and OPMN Configuration"
- Section 9.1.5, "Update the WEBHOST Configuration"

- Section 9.1.6, "Validate the WEBHOST and Administration Server Configuration Changes"

9.1.1 Enabling a Virtual IP Address on IDMHOST1

The Oracle WebLogic Administration Server must be configured to listen on a virtual IP address to enable it to seamlessly failover from one host to another. In case of a failure, the Administration Server, along with the virtual IP address, can be migrated from one host to another.

However, before the Administration Server can be configured to listen on a virtual IP address, one of the network interface cards on the host running the Administration Server must be configured to listen on this virtual IP address. The steps to enable a virtual IP address are completely dependent on the operating system.

Follow the steps in this section to enable a virtual IP address on IDMHOST1. In a UNIX environment, the commands must be run as the `root` user:

1. On IDMHOST1, run the `ifconfig` command to get the value of the netmask. In a UNIX environment, run this command as the `root` user. For example:

```
[root@idmhost1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:43:D7:5B:06
          inet addr:139.185.140.51  Bcast:139.185.140.255  Mask:255.255.255.0
          inet6 addr: fe80::211:43ff:fed7:5b06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10626133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10951629 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4036851474 (3.7 GiB)  TX bytes:2770209798 (2.5 GiB)
          Base address:0xecc0 Memory:dfae0000-dfb00000
```

2. On IDMHOST1, bind the virtual IP address to the network interface card using `ifconfig`. The syntax and usage for the `ifconfig` command is shown below. In a UNIX environment, run this command as the `root` user. Use a netmask value that was obtained in Step 1.

```
/sbin/ifconfig networkCardInterface VirtualIPAddress netmask netMask
```

   For example:

```
/sbin/ifconfig eth0:1 139.185.140.200 netmask 255.255.255.0
```

3. Update the routing tables using `arping`. In a UNIX environment, run this command as the `root` user.

```
/sbin/arping -q -U -c 3 -I networkCardInterface VirtualIpAddress
```

   For example:

```
/sbin/arping -q -U -c 3 -I eth0 139.185.140.200
```

9.1.2 Create a Machine for the Administration Server

Create a new machine and assign the Administration Server to the new machine using the WebLogic Administration Console:

1. Log into the Administration Server Console.
2. In the Change Center, click **Lock and Edit** to enable configuration changes.

3. In the Environment section of the Home page, click **Machines**.
4. On the Summary of Machines page, select the Machine that is associated with the Administration Server from under the Machines table and click **Clone**. For example: `idmhost1.mycompany.com`
5. On the Clone a Machine page, enter the Name for the Machine under the Machine Identity section and click **OK**. For example, enter `IDMHOST-VIP` as the machine name.
6. On the Summary of Machines page, click the newly created machine link.
7. On the Settings page for the IDMHOST-VIP machine, select the Servers tab.
8. Click the **Add** button under the Servers table.
9. On the Add a Server to Machine page, choose the **Select an existing server, and associate it with this machine** option.
10. Choose the Administration Server from the drop down menu.
11. Click **Finish** to associate the Administration Server with the Machine.
12. Navigate back to the Summary of Machines page and select the Machine that is associated with the `WLS_ODS1` Managed Server. For example: `idmhost1.mycompany.com`
13. On the Settings page for the `idmhost1.mycompany.com` machine, select the Node Managers tab.
14. Update the Listen Address to `IDMHOST1` and save the changes.
15. Click **Activate All Changes** under the Change Center to apply all the changes.

9.1.3 Enable the Administration Server to Listen on the Virtual IP Address

To enable the Administration Server to listen on the virtual IP address, follow these steps:

1. Log into the Administration Server Console.
2. In the Change Center, click **Lock and Edit** to enable configuration changes.
3. In the Environment section of the Home page, click **Servers**.
4. On the Summary of Servers page, click the **AdminHost** link.
5. Update the Listen Address for the Administration Server with the virtual IP enabled. Specify `idmhost-vip.mycompany.com` for the Listen Address.
6. Save these changes, and then activate the changes.
7. Stop and then restart the Administration Server.

   See the "Starting and Stopping Oracle Fusion Middleware" chapter of the *Oracle Fusion Middleware Administrator's Guide* for information on starting and stopping WebLogic Servers.

9.1.4 Update Enterprise Manager Agent and OPMN Configuration

The Oracle Enterprise Manager Agent and the OPMN configurations for the Oracle instances listed in the following table must be updated with the virtual IP address. This is to enable them to successfully connect to the Administration Server.

Oracle Instance Name	Oracle Instance Path	Host Name
OID_INSTANCE1	*ORACLE_BASE*/admin/oid_instance1	oidhost1.mycompany.com
OID_INSTANCE2	*ORACLE_BASE*/admin/oid_instance2	oidhost2.mycompany.com
OVD_INSTANCE1	*ORACLE_BASE*/admin/ovd_instance1	ovdhost1.mycompany.com
OVD_INSTANCE2	*ORACLE_BASE*/admin/ovd_instance2	ovdhost2.mycompany.com
ADMIN_INSTANCE	*ORACLE_BASE*/admin/admin_instance	idmhost1.mycompany.com
IDM_INSTANCE1	*ORACLE_BASE*/admin/idm_instance1	idmhost1.mycompany.com
IDM_INSTANCE2	*ORACLE_BASE*/admin/idm_instance2	idmhost2.mycompany.com

Follow these steps to update the Oracle Enterprise Manager Agent and OPMN configuration for all the Oracle instances listed in the table above:

1. Update the `emdWalletSrcURL` and `REPOSITORY_URL` properties with the virtual IP address in the `emd.properties` file, which is located under the *`ORACLE_INSTANCE`*`/EMAGENT/`*`emAgentDir`*`/sysman/config/`directory:

   ```
   emdWalletSrcUrl=http://IDMHOST-VIP:7001/em/wallets/emd
   REPOSITORY_URL=http://IDMHOST-VIP:7001/em/upload
   ```

2. Update the `adminHost` property with the virtual IP address in the `instance.properties` file, which is located under the *`ORACLE_INSTANCE`*`/config/OPMN/opmn` directory.

3. Stop and restart the Oracle Enterprise Manager Agent as follows:

   ```
   opmnctl stopproc ias-component=EMAGENT
   opmnctl startproc ias-component=EMAGENT
   ```

9.1.5 Update the WEBHOST Configuration

The `mod_wl_ohs` configuration on the WEBHOST1 and WEBHOST2 must be updated with the virtual IP address. This will enable the Oracle HTTP Server instances to properly route traffic to applications deployed on the Administration Server.

Update the `WebLogicHost` directive in the `mod_wl_ohs.conf` file with the virtual IP address as in the steps below. The `mod_wl_ohs.conf` file is located under the *`ORACLE_INSTANCE`*`/config/OHS/`*`componentName`* directory on WEBHOST1 and WEBHOST2.

1. Update the Administration Console and Oracle Enterprise Manager Fusion Middleware Control application-related directives in the `mod_wl_ohs.conf` file on WEBHOST1 and WEBHOST2 as shown below:

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

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

```
<Location /em>
SetHandler weblogic-handler
WebLogicHost idmhost-vip.mycompany.com
WeblogicPort 7001
</Location>
```

2. Save the `mod_wl_ohs.conf` file and restart the Oracle HTTP Server processes on WEBHOST1 and WEBHOST2 as shown below:

   ORACLE_INSTANCE`/bin/opmnctl restartproc ias-component=ohs1`

9.1.6 Validate the WEBHOST and Administration Server Configuration Changes

Validate that the configuration changes made so far to the Administration Server, WEBHOST1, and WEBHOST2 were successful by following these steps:

1. Open a web browser.
2. To validate the configuration changes made to WEBHOST1 and WEBHOST2, access the WebLogic Server Administration Console and the Oracle Enterprise Manager Fusion Middleware Control at the following URLs:
   - WebLogic Server Administration Console:

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

   - Oracle Enterprise Manager Fusion Middleware Control:

     `http://admin.mycompany.com:7001/em`

3. To validate the configuration changes made to the Administration Server, access the WebLogic Server Administration Console and the Oracle Enterprise Manager Fusion Middleware Control at the following URLs:
   - WebLogic Server Administration Console:

     `http://idmhost-vip.mycompany.com:7001/console`

   - Oracle Enterprise Manager Fusion Middleware Control:

     `http://idmhost-vip.mycompany.com:7001/em`

Log into these consoles using the `weblogic_idm` user credentials and verify that all the components apppear in the Oracle Enterprise Manager Fusion Middleware Control. Specifically, check to see if the non-J2EE components (for example, Oracle Internet Directory, Oracle Virtual Directory, and Oracle HTTP Server) appear in the console.

9.2 Provisioning the Administration Server and Fusion Middleware Control on IDMHOST2

Follow these steps to provision the WebLogic Administration Server and Oracle Enterprise Manager Fusion Middleware Control on IDMHOST2:

1. Stop the Administration Server running on IDMHOST1.

   See the "Starting and Stopping Oracle Fusion Middleware" chapter of the *Oracle Fusion Middleware Administrator's Guide* for information on starting and stopping WebLogic Servers.

2. For all the Oracle instances listed in the table in Section 9.1.4, "Update Enterprise Manager Agent and OPMN Configuration," stop the Oracle Enterprise Manager Agent as follows:

   ```
   opmnctl stopproc ias-component=EMAGENT
   ```

3. Copy the *DOMAIN_HOME*/servers/AdminServer directory from IDMHOST1 to IDMHOST2 as shown below:

   ```
   scp -rp DOMAIN_HOME/servers/AdminServer user@idmhost2://DOMAIN_
   HOME/servers/AdminServer
   ```

4. Copy the *DOMAIN_HOME*/sysman directory from IDMHOST1 to IDMHOST2 as shown below:

   ```
   scp -rp DOMAIN_HOME/sysman user@idmhost2://DOMAIN_HOME/sysman
   ```

5. Create the directory structure shown below on IDMHOST2:

   ```
   mkdir -p APPLICATIONS_HOME/DOMAIN_NAME
   ```

6. Copy the *APPLICATIONS_HOME*/*DOMAIN_NAME*/em.ear file from IDMHOST1 to IDMHOST2 as shown below:

   ```
   scp -rp APPLICATIONS_HOME/DOMAIN_NAME/em.ear user@idmhost2://APPLICATIONS_
   HOME/DOMAIN_NAME/em.ear
   ```

7. Copy the *DOMAIN_HOME*/opmn directory from IDMHOST1 to IDMHOST2 as shown below:

   ```
   scp -rp DOMAIN_HOME/opmn user@idmhost2://DOMAIN_HOME/opmn
   ```

8. Copy the *DOMAIN_HOME*/bin/setDomainEnv.sh file from IDMHOST1 to IDMHOST2 as shown below:

   ```
   scp -rp DOMAIN_HOME/bin/setDomainEnv.sh user@idmhost2://DOMAIN_HOME/bin
   ```

9. For all the Oracle instances listed in the table in Section 9.1.4, "Update Enterprise Manager Agent and OPMN Configuration," start the Oracle Enterprise Manager Agent as follows:

   ```
   opmnctl startproc ias-component=EMAGENT
   ```

Note: If a user is assigned the Admin role after an Administration Server failover to IDMHOST2, when a failback to IDMHOST1 is performed, the role changes made on IDMHOST2 are not reflected on IDMHOST1.

To fix this issue:

1. Copy the *DOMAIN_HOME*/servers/AdminServer/data/ldap directory from IDMHOST2 to IDMHOST1.
2. Stop and start the Administration Server on IDMHOST1.

9.3 Validating Administration Server and Oracle Fusion Middleware Control Failover on IDMHOST2

Follow these steps to validate the failover of the WebLogic Administration Server and Oracle Enterprise Manager Fusion Middleware Control from IDMHOST1 to IDMHOST2:

1. Make sure that the Administration Server is not running on IDMHOST1. If it is running, use the WebLogic Administration Console to stop the Administration Server on IDMHOST1.
2. Make sure that the virtual IP has been disabled on IDMHOST1. If it is not disabled, then disable it using the `ifconfig` command. In a UNIX environment, run this command as the `root` user. For example:

   ```
   /sbin/ifconfig networkCardInterface down
   ```

3. Enable the virtual IP on IDMHOST2 using the `ifconfig` command. The syntax and usage for the `ifconfig` command is shown below. In a UNIX environment, run the `ifconfig` command as the `root` user.

   ```
   /sbin/ifconfig networkCardInterface IPAddress netmask netMask
   ```

   For example:

   ```
   /sbin/ifconfig eth0:1 139.185.140.200 netmask 255.255.255.0
   ```

4. Update the routing tables using the `arping` command. In a UNIX environment, run the `arping` command as the `root`. user.

   ```
   /sbin/arping -q -U -c 3 -I networkCardInterface VirtualIPAddress
   ```

   For example:

   ```
   /sbin/arping -q -U -c 3 -I eth0 139.185.140.200
   ```

5. Start the WebLogic Administration Server on IDMHOST2 using the `startweblogic.sh` script located under the *MW_HOME*`/user_projects/domains/IDMDomain/bin` directory.
6. After the Administration Server starts up, validate that you can access the WebLogic Server Administration Console and the Oracle Enterprise Manager Fusion Middleware Control using the virtual IP. For example:
   - To access the WebLogic Administration Server Console using the virtual IP address, open a web browser and enter this URL:

     ```
     http://idmhost-vip.mycompany.com:7777/console
     ```

   - To access the Oracle Enterprise Manager Fusion Middleware Control using the virtual IP address, open a web browser and enter this URL:

     ```
     http://idmhost-vip.mycompany.com:7777/em
     ```

   - To access the WebLogic Administration Server Console using the virtual hostname, open a web browser and enter this URL:

     ```
     http://admin.mycompany.com:7777/console
     ```

   - To access the Oracle Enterprise Manager Fusion Middleware Control using the virtual hostname, open a web browser and enter this URL:

     ```
     http://admin.mycompany.com:7777/em
     ```

Log into each by specifying the credentials for the `weblogic_idm` user.

10

Managing Enterprise Deployments

This chapter provides information about managing the Identity Management enterprise deployment you have set up.

This chapter includes the following topics:

10.1 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity Management enterprise deployment described in this manual.

10.1.1 Monitoring Oracle Internet Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Internet Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each individual Oracle Internet Directory instance (for example, oid1, oid2), its status, host name, and CPU usage percentage. A green arrow in the Status column indicates that the instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Internet Directory instance to view the home page for that instance.
3. The home page for an instance displays metrics for the instance such as performance, load, security, response, CPU utilization %, and memory utilization %.

10.1.1.1 Oracle Internet Directory Component Names Assigned by Oracle Identity Management Installer

When you perform an Oracle Internet Directory installation using Oracle Identity Management 11*g* Installer, the default component name that the installer assigns to the Oracle Internet Directory instance is oid1. You cannot change this component name.

The instance specific configuration entry for this Oracle Internet Directory instance is "cn=oid1, cn=osdldapd, cn=subconfigsubentry".

If you perform a second Oracle Internet Directory installation on another computer and that Oracle Internet Directory instance uses the same database as the first instance, the installer detects the previously installed Oracle Internet Directory instance on the other computer using the same Oracle database, so it gives the second Oracle Internet Directory instance a component name of oid2.

The instance specific configuration entry for the second Oracle Internet Directory instance is "cn=oid2, cn=osdldapd, cn=subconfigsubentry". Any change of properties in the entry "cn=oid2, cn=osdldapd, cn=subconfigsubentry" will not affect the first instance (oid1).

If a third Oracle Internet Directory installation is performed on another computer and that instance uses the same database as the first two instances, the installer gives the third Oracle Internet Directory instance a component name of oid3, and so on for additional instances on different hosts that use the same database.

Note that the shared configuration for all Oracle Internet Directory instances is "cn=dsaconfig, cn=configsets,cn=oracle internet directory". Any change in this entry will affect all the instances of Oracle Internet Directory.

This naming scheme helps alleviate confusion when you view your domain using Oracle Enterprise Manager by giving different component names to your Oracle Internet Directory instances.

10.1.2 Monitoring Oracle Virtual Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Virtual Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each instance of the Oracle Virtual Directory application (for example, ovd1, ovd2), its status, and host name. A green arrow in the Status column indicates that the Oracle Virtual Directory instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Virtual Directory instance to view the home page for that instance.
3. The home page for an instance displays metrics and configurations for the instance such as:
   - Oracle Virtual Directory status - A green arrow next to the Oracle Virtual Directory instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.
   - Current Load - This indicates the current work load of this Oracle Virtual Directory instance. It includes three metrics: Open Connections, Distinct Connected Users, and Distinct Connected IP Addresses.

- Average Response Time Metric - This displays the average time (in milliseconds) to complete an LDAP search request.
- Operations Metric - This displays the average number of LDAP search requests finished per millisecond.
- Listeners - This table lists the listeners configured for this Oracle Virtual Directory instance to provide services to clients.
- Adapters - This table lists existing adapters configured with the Oracle Virtual Directory instance. Oracle Virtual Directory uses adapters to connect to different underlying data repositories.
- Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the system resources consumed by the Oracle Virtual Directory instance.

10.1.3 Monitoring Oracle Directory Integration Platform

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Directory Integration Platform, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each instance of the Oracle Directory Integration Platform application (all have the name DIP (11.1.1.1.0)), its status, and host name. Each Oracle Directory Integration Platform instance is deployed in a different Managed Server). A green arrow in the Status column indicates that the Oracle Directory Integration Platform instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Directory Integration Platform instance to view the home page for that instance.
3. The home page for an instance displays metrics for the instance such as:
   - Oracle Directory Integration Platform status - A green arrow next to the Oracle Directory Integration Platform instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.
   - DIP Component Status - This table includes these metrics:
     - Quartz Scheduler - This indicates whether tasks can be scheduled for synchronization or not. A green arrow indicates the scheduler is up and a red arrow indicates that the scheduler is down.
     - Mbeans - This indicates whether profile management is available to the user or not. A green arrow indicates profile management is available and a red arrow indicates profile management is unavailable.
   - Synchronization Profiles - This shows registered profiles and their execution status. In a high availability deployment, all the instances will show the same list of profiles.
   - Provisioning Profiles- This shows registered provisioning profiles and their execution status. In a high availability deployment, all the instances will show the same list of profiles.

- Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the resource usage by the Oracle Directory Integration Platform instance.

10.1.4 Monitoring Oracle Access Manager

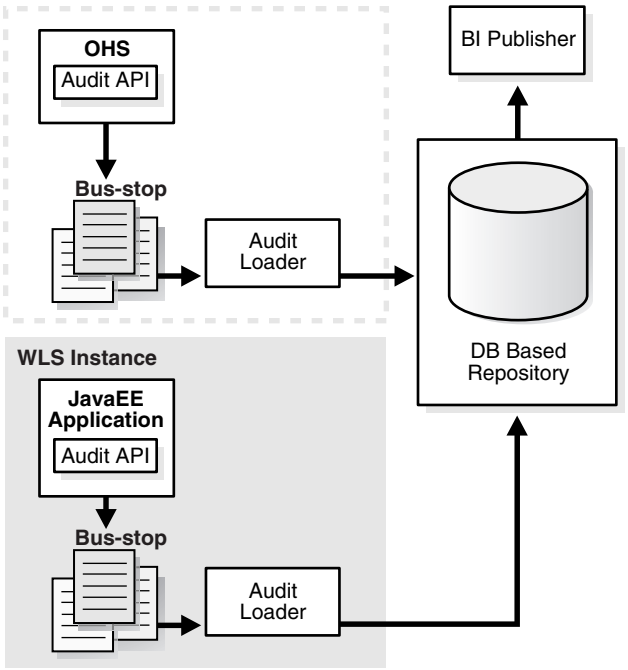
Oracle Enterprise Manager Grid Control can be used to perform monitoring of Oracle Access Manager. For details, see the "Identity Management" chapter of *Oracle Enterprise Manager Concepts*.

10.2 Auditing Identity Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications will be 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 10–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 10–1 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

runtime, applications may call these APIs where appropriate to audit the necessary information about a particular event happening in the application code. The interface allows 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 allows 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 will grow overtime. 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 (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 allow 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 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 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 will be 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.

10.3 Scaling Enterprise Deployments

The reference enterprise topology discussed in this manual is highly scalable. It can be scaled up and or scaled out. When the topology is scaled up, a new server instance is added to a node already running one or more server instances. When the topology is scaled out, new servers are added to new nodes.

10.3.1 Scaling Up the Topology

The Oracle Identity Management topology described in the guide has three tiers: the directory tier, application tier and web tier. The components in all the three tiers can be scaled up by adding a new server instance to a node that already has one or more server instances running.

10.3.1.1 Scaling Up the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled up on one or both the nodes.

10.3.1.1.1 Scaling Up Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Internet Directory instance.

To add a new Oracle Internet Directory instance to either Oracle Internet Directory node, follow the steps in Section 4.5.3, "Installing an Additional Oracle Internet Directory" with the following variations:

1. In step 2 and step 4, choose ports other than 389 and 636 since these ports are being used by the existing Oracle Internet Directory instance on the node.
2. In step 5, instead of running the Oracle Identity Management 11*g* Installer, use the Oracle Fusion Middleware 11*g* Identity Management Configuration Wizard since the ORACLE_HOME already exists. Run the `config.sh` script under the *`ORACLE_HOME`*`/bin` directory to bring up the configuration wizard and follow the remaining steps to add a new Oracle Internet Directory instance to the node.
3. The screens in steps 6, 8, 9, 18, and 19 in Section 4.5.3, "Installing an Additional Oracle Internet Directory" are related to a new install and will not be shown since the ORACLE_HOME is being shared.
4. Follow the steps in Section 4.5.4, "Registering Oracle Internet Directory with the WebLogic Server Domain" to register the new Oracle Internet Directory instance

with the WebLogic Domain. Use the location for the new Oracle Internet Directory instance as the value for ORACLE_INSTANCE.

5. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

10.3.1.1.2 Scaling Up Oracle Virtual Directory The directory tier has two nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Virtual Directory instance.

To add a new Oracle Virtual Directory instance to either Oracle Virtual Directory node, follow the steps in Section 4.6.2, "Installing an Additional Oracle Virtual Directory" with the following variations:

1. In step 2 and step 4, choose ports other than 6501 and 7501 since these ports are being used by the existing Oracle Virtual Directory instance on the node.
2. In step 6, instead of running the Oracle Identity Management 11*g* Installer, use the Oracle Fusion Middleware 11*g* Identity Management Configuration Wizard since the ORACLE_HOME already exists. Run the `config.sh` script under the *`ORACLE_HOME`*`/bin` directory to bring up the configuration wizard and follow the remaining steps to add a new Oracle Virtual Directory instance to the node.
3. The screens in steps 7, 9, 10, 16 and 17 in Section 4.6.2, "Installing an Additional Oracle Virtual Directory" are related to a new install and will not be shown since the ORACLE_HOME is being shared.
4. Follow the steps in Section 4.6.3, "Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain" to register the new Oracle Virtual Directory instance with the WebLogic Domain. Use the location for the new Oracle Virtual Directory instance as the value for ORACLE_INSTANCE.
5. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

10.3.1.2 Scaling Up the Application Tier

The application tier has two nodes (IDMHOST1 and IDMHOST2) running Managed Servers for Oracle Directory Integration Platform and Oracle Directory Services Manager, two nodes (OAMHOST1 and OAMHOST2) running the Oracle Access Manager Identity Server and Access Server, and an Administration node (OAMADMINHOST) running an instance of the Oracle Access Manager WebPass, Policy Manager, WebGate and Oracle HTTP Server.

10.3.1.2.1 Scaling Up Oracle Directory Integration Platform and Oracle Directory Services Manager The application tier already has a node (IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager components. The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management Home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for the Oracle Oracle Directory Integration Platform and Oracle Directory Services Manager components.

Follow the steps in Section 5.2, "Expanding the DIP and ODSM Cluster" with the following variations to scale up the topology for Oracle Directory Integration Platform and Oracle Directory Services Manager:

1. Use the Oracle Identity Management Configuration Assistant to scale up the topology. Run the `config.sh` script under the *ORACLE_HOME*`/bin` directory to bring up the configuration assistant.
2. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in Section 6.4, "Configuring Oracle HTTP Server with the Load Balancer" and Section 6.5, "Configuring Oracle HTTP Server for Virtual Hosts" to complete this task.

10.3.1.3 Scaling Up Oracle Access Manager

With Oracle Access Manager, the new server instances need to be installed under a separate ORACLE_HOME location. Sharing ORACLE_HOMEs between instances of Oracle Access Manager components is not supported.

To scale up the Identity Server, follow the instructions in Section 7.3.1.2, "Installing the Second Identity Server on OAMHOST2."

To scale up the Access Server, follow the instructions in Section 7.4.2.2, "Starting the Access Server Installation."

To scale up the WebPass, follow the instructions in Section 7.3.3, "Installing WebPass on OAMADMINHOST."

To scale up the WebGate, follow the instructions in Section 7.4.3, "Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2."

10.3.1.4 Scaling Up the Web Tier

The web tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance. To scale up the Oracle HTTP Server, follow the steps in Section 6.2, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2" with the following variations:

1. Use the Oracle Fusion Middleware 11*g* Web Tier Utilities Configuration Wizard to scale up the topology. Run the `config.sh` script under the *ORACLE_HOME*`/bin` directory to bring up the configuration wizard and follow the remaining steps to create a new instance of the Oracle HTTP Server.
2. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

10.3.2 Scaling Out the Topology

In scaling out a topology, new servers are added to new nodes. The components in all three tiers of the Oracle Identity Management topology described in this manual can be scaled out by adding a new server instance to a new node.

10.3.2.1 Scaling Out the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled out by adding new nodes to the directory tier.

10.3.2.1.1 Scaling Out Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The OID instances can be scaled out by adding a new node to the

existing Oracle Internet Directory cluster. To scale out Oracle Internet Directory instances, follow these steps:

1. Follow the steps in Section 4.5.3, "Installing an Additional Oracle Internet Directory" to add a new node running Oracle Internet Directory.
2. Follow the steps in Section 4.5.4, "Registering Oracle Internet Directory with the WebLogic Server Domain" to register the new Oracle Internet Directory instance with the WebLogic domain.
3. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

10.3.2.1.2 Scaling Out Oracle Virtual Directory The directory tier has two nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. Oracle Virtual Directory can be scaled out by adding a new node configured to run Oracle Virtual Directory to the directory tier. To scale out Oracle Virtual Directory instances, follow these steps:

1. Follow the steps in Section 4.6.2, "Installing an Additional Oracle Virtual Directory" to add a new node running Oracle Virtual Directory.
2. Follow the steps in Section 4.6.3, "Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain" to register the new Oracle Virtual Directory instance with the WebLogic domain.
3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

10.3.2.2 Scaling Out the Application Tier

The application tier has two nodes (IDMHOST1 and IDMHOST2) running Managed Servers for Oracle Directory Integration Platform and Oracle Directory Services Manager, two nodes (OAMHOST1 and OAMHOST2) running the Oracle Access Manager Identity Server and Access Server, and an Administration node (OAMADMINHOST) running an instance of the Oracle Access Manager WebPass, Policy Manager, WebGate and Oracle HTTP Server.

10.3.2.2.1 Scaling Out Oracle Directory Integration Platform and Oracle Directory Services Manager The application tier has two nodes (IDMHOST1 and IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager. The Oracle Directory Integration Platform and Oracle Directory Services Manager instances can be scaled out by adding a new node with a Managed Server to the existing cluster. To scale out DIP and ODSM instances, follow the steps below:

1. Follow the steps in Section 5.2, "Expanding the DIP and ODSM Cluster" to scale out the Oracle Directory Integration Platform and Oracle Directory Services Manager instances in the topology.
2. Reconfigure the Oracle HTTP Server module with the new Managed Server. See Section 6.6, "Configuring mod_wl_ohs for Oracle WebLogic Server Clusters" for the instructions to complete this task.

10.3.2.2.2 Scaling Out Oracle Access Manager With Oracle Access Manager, the new server instances need to be installed under a separate ORACLE_HOME location. Sharing ORACLE_HOMEs between instances of Oracle Access Manager components is not supported.

To scale out the Identity Server, follow the instructions in Section 7.3.1.2, "Installing the Second Identity Server on OAMHOST2."

To scale out the Access Server, follow the instructions in Section 7.4.2.2, "Starting the Access Server Installation."

To scale out the WebPass, follow the instructions in Section 7.3.3, "Installing WebPass on OAMADMINHOST."

To scale out the WebGate, follow the instructions in Section 7.4.3, "Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2."

10.3.2.3 Scaling Out the Web Tier

The web tier has two nodes each running an instance of the Oracle HTTP Server. The Oracle HTTP Server components can be scaled out by adding a new node configured to run Oracle HTTP Server to the web tier. To scale out Oracle HTTP Server, follow these steps:

1. Follow the steps in Section 6.2, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2" to scale out the Oracle HTTP Server instances in the topology.
2. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server node.

10.4 Performing Backups and Recoveries

Table 10–1 shows the static artifacts to back up in the 11*g* Oracle Identity Management enterprise deployment.

Table 10–1 Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	RAC database hosts: INFRADBHOST1 INFRADBHOST2	User Defined	Directory Tier
MW_HOME (OID)	OIDHOST1 OIDHOST2	MW HOME: /u01/app/oracle/product/fmw ORACLE HOME: /u01/app/oracle/product/fmw/idm on both the OIDHOST1 and OIDHOST2	Directory Tier
MW_HOME (OVD)	OVDHOST1 OVDHOST2	MW HOME: /u01/app/oracle/product/fmw ORACLE HOME: /u01/app/oracle/product/fmw/idm on both the OVDHOST1 and OVDHOST2	Directory Tier
MW_HOME (DIP, ODSM, Admin Server)	IDMHOST1 IDMHOST2	FMW HOME: /u01/app/oracle/product/fmw DIP/ODSM ORACLE HOME: /u01/app/oracle/product/fmw/idm on both IDMHOST1 and IDMHOST2 ADMIN SERVER ORACLE HOME: /u01/app/oracle/product/fmw/idm on both IDMHOST1 and IDMHOST2	Application Tier

Table 10–1 (Cont.) Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier
MW_HOME (OHS)	WEBHOST1 WEBHOST2	MW HOME: /u01/app/oracle/product/fmw ORACLE HOME: /u01/app/oracle/product/fmw/web on WEBHOST1 ORACLE HOME: /u01/app/oracle/product/fmw/web on WEBHOST2	Web Tier
OAMADMINHOST (used for OAM administration)	OAMADMINHOST	MW HOME: /u01/app/oracle/product/fmw OHS ORACLE HOME: /u01/app/oracle/product/fmw/web WEBPASS HOME: /u01/app/oracle/product/fmw/oam/webcomponents/identity POLICY MANAGER HOME: /u01/app/oracle/product/fmw/oam/webcomponents/access WEBGATE HOME: /u01/app/oracle/product/fmw/oam/webgate	Application Tier
OAM	OAMHOST1 OAMHOST2	ORACLE ACCESS MANAGER HOME: /u01/app/oracle/product/fmw/oam IDENTITY SERVER HOME: /u01/app/oracle/product/fmw/oam/identity ACCESS SERVER HOME: /u01/app/oracle/product/fmw/oam/access	Application Tier
Install Related Files	Each host	OraInventory: ORACLE_BASE/orainventory /etc/oratab, /etc/oraInst.loc <user_home>/bea/beahomelist (on hosts where WebLogic Server is installed) Windows registry: (HKEY_LOCAL/MACHINE/Oracle)	Not applicable.

Table 10–2 shows the runtime artifacts to back up in the 11*g* Oracle Identity Management enterprise deployment:

Table 10–2 Runtime Artifacts to Back Up in the Identity Management Enterprise Deployments

Type	Host	Location	Tier
DOMAIN HOME	RAC database hosts: IDMHOST1 IDMHOST2	MW_HOME/user_projects/domains/IDMDomain on both IDMHOST1 and IDMHOST2	Application Tier
Application Artifacts (ear and war files)	IDMHOST1 IDMHOST2	Look at all the deployments, including Oracle Directory Integration Platform and Oracle Directory Services Manager, through the WebLogic Server Administration Console to identity all the application artifacts.	Application Tier
INSTANCE HOME (OHS)	WEBHOST1 WEBHOST2	OHS INSTANCE HOME on WEBHOST1: /u01/app/oracle/admin/ohs_inst1 OHS INSTANCE HOME on WEBHOST2: /u01/app/oracle/admin/ohs_inst2	Web Tier
INSTANCE HOME (OHS)	OAMADMINHOST	OHS INSTANCE HOME on WEBHOST1: /u01/app/oracle/admin/ohs_inst/oamAdmin_ohs	Application Tier

Table 10–2 (Cont.) Runtime Artifacts to Back Up in the Identity Management Enterprise Deployments

Type	Host	Location	Tier
OID INSTANCE HOME	OIDHOST1 OIDHOST2	OID INSTANCE HOME on OIDHOST1: /u01/app/oracle/admin/oid_inst1 OID INSTANCE HOME on OIDHOST2: /u01/app/oracle/admin/oid_inst2	Directory Tier
OVD INSTANCE HOME	OVDHOST1 OVDHOST2	OVD INSTANCE HOME on OVDHOST1: /u01/app/oracle/admin/ovd_inst1 OVD INSTANCE HOME on OVDHOST2: /u01/app/oracle/admin/ovd_inst2	Directory Tier
RAC Databases	INFRADBHOST1 INFRADBHOST2	User defined	Directory Tier
OAM	OAMHOST1 OAMHOST2 OAMADMINHOST	All the configurations are within the respective home directories described in this table. There are no instance homes.	Application Tier

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

10.5 Patching Enterprise Deployments

This section describes how to patch an Oracle Fusion Middleware patch file and how to patch Oracle Identity Management components with minimal down time.

10.5.1 Patching an Oracle Fusion Middleware Source File

For information on patching an Oracle Fusion Middleware source file, see the *Oracle Fusion Middleware Administrator's Guide*.

10.5.2 Patching Identity Management Components

To patch Oracle Identity Management components with minimal down time, it is recommended that you follow these guidelines:

1. Route the LDAP traffic from OIDHOST1 and OVDHOST1 to OIDHOST2 and OVDHOST2.
2. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST1 or OVDHOST1).
3. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
4. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
5. Test the patch.
6. Route the traffic to OIDHOST1 or OVDHOST1 again.
7. Verify the applications are working properly.
8. Route the LDAP traffic on OIDHOST2 and OVDHOST2 to OIDHOST1 and OVDHOST1.
9. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST2 or OVDHOST2).

10. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
11. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
12. Test the patch.
13. Route the traffic to both hosts on which the patch has been applied (OIDHOST1 and OIDHOST2, or OVDHOST1 and OVDHOST2).

10.6 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity Management enterprise deployment described in this manual.

10.6.1 Troubleshooting Oracle Internet Directory

This section describes some of the common problems that can arise with Oracle Internet Directory and the actions you can take to resolve the problem.

Problem

The Oracle Internet Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Internet Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to Oracle Internet Directory server

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

The LDAP application is receiving LDAP Error 53 (DSA Unwilling to Perform). When one of the database nodes goes down during the middle of the LDAP transaction, the Oracle Internet Directory server sends error 53 to the LDAP client

Solution

To see why the Oracle Internet Directory database node went down, see the Oracle Internet Directory logs in this location:

ORACLE_INSTANCE/diagnostics/logs/OID/oidldapd01s*.log

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

10.6.2 Troubleshooting Oracle Virtual Directory

This section describes some of the common problems that can arise with Oracle Virtual Directory and the actions you can take to resolve the problem:

Problem

The Oracle Virtual Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Virtual Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to the Oracle Virtual Directory server.

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

10.6.3 Troubleshooting Oracle Directory Integration Platform

This section describes some of the common problems that can arise with Oracle Directory Integration Platform and the actions you can take to resolve the problem.

Problem

The instance is not working properly.

Solution

Check the respective log of the instance. For example, if the instance deployed in wls_ods1 is not running, then check the wls_ods1-diagnostic.log file.

Problem

Exceptions similar to the following are seen in Managed Server log files running the Oracle Directory Integration Platform application during a RAC failover:

```
RuntimeException:
[2008-11-21T00:11:10.915-08:00] [wls_ods] [ERROR] []
[org.quartz.impl.jdbcjobstore.JobStoreTX] [tid: 25] [userId: <anonymous>]
```

```
[ecid: 0000Hqy69UiFW7V6u3FCEH199aj0000009,0] [APP: DIP] ClusterManager: Error
managing cluster: Failed to obtain DB connection from data source
'schedulerDS': java.sql.SQLException: Could not retrieve datasource via JNDI
url 'jdbc/schedulerDS' java.sql.SQLException: Cannot obtain connection:
driverURL = jdbc:weblogic:pool:schedulerDS, props =
{EmulateTwoPhaseCommit=false, connectionPoolID=schedulerDS,
jdbcTxDataSource=true, LoggingLastResource=false,
dataSourceName=schedulerDS}.[[
Nested Exception: java.lang.RuntimeException: Failed to setAutoCommit to true
for pool connection

AuthenticationException while connecting to OID:
[2008-11-21T00:12:08.812-08:00] [wls_ods] [ERROR] [DIP-10581] [oracle.dip]
[tid: 11] [userId: <anonymous>] [ecid: 0000Hqy6m54FW7V6u3FCEH199apO000000,0]
[APP: DIP] DIP was not able to get the context with the given details {0}[[
javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid
Credentials]
```

Most of the exceptions will be related to the scheduler or LDAP, for example:

1. Could not retrieve datasource via JNDI url 'jdbc/schedulerDS' java.sql.SQLException.

2. javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]

Solution

During a RAC failover, exceptions are seen in the Managed Server log files running the Oracle Directory Integration Platform application. These errors are thrown when the multi data sources configured on the WebLogic Server platform try to verify the health of the RAC database instances during failover. These are innocuous errors and can be ignored. The Oracle Directory Integration Platform application will recover and begin to operate normally after a lag of one or two minutes. For a RAC failover, there will be no Oracle Directory Integration Platform down time if one instance is running at all times.

10.6.4 Troubleshooting Oracle Directory Services Manager

This section describes some of the common problems that can arise with Oracle Directory Services Manager and the actions you can take to resolve the problem.

After you have logged into Oracle Directory Services Manager, you can connect to multiple directory instances from the same browser window.

Avoid using multiple windows of the same browser program to connect to different directories at the same time. Doing so can cause a Target unreachable error.

You can log into the same Oracle Directory Services Manager instance from different browser programs, such as Internet Explorer and Firefox, and connect each to a different directory instance.

If you change the browser language setting, you must update the session in order to use the new setting. To update the session, either disconnect the current server connection, refresh the browser page (either reenter the Oracle Directory Services Manager URL in the URL filed and press enter or press F5) and reconnect to the same server, or quit and restart the browser.

Problem

You attempt to invoke Oracle Directory Services Manager from Oracle Enterprise Manager Fusion Middleware Control by selecting Directory Services Manager from

the Oracle Internet Directory menu in the Oracle Internet Directory target, then Data Browser, Schema, Security, or Advanced.

Oracle Directory Services Manager does not open. You might see an error message.

Solution

This is probably an installation problem. See Oracle Fusion Middleware Installation Guide for Oracle Identity Management.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You will see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.
2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.
3. Make a connection to an Oracle Internet Directory server.
4. Work with the Oracle Internet Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.
5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.
6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Internet Directory.
7. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.
2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.
3. Re-establish a new connection to the Oracle Internet Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to Oracle Internet Directory and displays the message LDAP Server is down.

Solution

In a High Availability configuration where Oracle Directory Services Manager is connected to Oracle Internet Directory through a load balancer, Oracle Directory Services Manager reports that the server is down during failover from one instance of Oracle Internet Directory to another. In other configurations, this message might indicate that Oracle Internet Directory has been shut down and restarted. In either case, the connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Internet Directory instance that is using a RAC database. Oracle Directory Services Manager might display the message

LDAP error code 53 - Function not implemented.

Solution

This error can occur during failover of the Oracle Database that the Oracle Internet Directory instance is using. The connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

Problem

You must perform the steps below to configure Oracle HTTP Server to route Oracle Directory Services Manager requests to multiple Oracle WebLogic Servers in a clustered Oracle WebLogic Server environment.

Solution

Perform these steps:

1. Create a backup copy of the Oracle HTTP Server's httpd.conf file. The backup copy will provide a source to revert back to if you encounter problems after performing this procedure.
2. Add the following text to the end of the Oracle HTTP Server's httpd.conf file and replace the variable placeholder values with the host names and Managed Server port numbers specific to your environment. Be sure to use the `<Location /odsm/ >` as the first line in the entry. Using `<Location /odsm/faces >` or `<Location /odsm/faces/odsm.jspx >` can distort the appearance of the Oracle Directory Services Manager interface.

   ```
   <Location /odsm/ >
   SetHandler weblogic-handler
   WebLogicCluster host-name-1:managed-server-port,host-name_2:managed_server_port
   </Location>
   ```

3. Stop, then start the Oracle HTTP Server to activate the configuration change.

> **Note:** Oracle Directory Services Manager loses its connection and displays a session time-out message if the Oracle WebLogic Server in the cluster that it is connected to fails. Oracle Directory Services Manager requests will be routed to the secondary Oracle WebLogic Server in the cluster that you identified in the httpd.conf file after you log back in to Oracle Directory Services Manager.

Problem

Attempting to access Oracle Directory Services Manager using a web browser fails.

Solution

- Verify the Oracle Virtual Directory server is running. The Oracle Virtual Directory server must be running to connect to it from Oracle Directory Services Manager.
- Verify you entered the correct credentials in the Server, Port, User Name and Password fields. You can execute an ldapbind command against the target Oracle Virtual Directory server to verify the server, user name, and password credentials.

- Verify you are using a supported browser. Oracle Directory Services Manager supports the following browsers:
  - Internet Explorer 7
  - Firefox 2.0.0.2 and 3.0
  - Safari 3.1.2 (desktop)
  - Google Chrome 0.2.149.30

  Note: While Oracle Directory Services Manager supports all of the preceding browsers, only Internet Explorer 7 and Firefox 2.0.0.2 are certified.

Problem

Oracle Directory Services Manager does not open after you attempt to invoke it from Oracle Enterprise Manager Fusion Middleware Control by selecting one of the options from the **Directory Services Manager** entry in the **Oracle Virtual Directory** menu in the Oracle Virtual Directory target.

Solution

This is probably an installation problem. See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You will see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.
2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.
3. Make a connection to an Oracle Virtual Directory server.
4. Work with the Oracle Virtual Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.
5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.
6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Virtual Directory. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.
2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.
3. Re-establish a new connection to the Oracle Virtual Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Virtual Directory instance that is using an Oracle RAC Database. Oracle Directory Services Manager might display the message `LDAP error code 53 - Function not implemented`.

Solution

This error can occur during failover of the Oracle Database that the Oracle Virtual Directory instance is using. The connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

10.6.5 Troubleshooting Oracle Access Manager

Most of the manuals in the Oracle Access Manager 10.1.4.3 documentation set include a Troubleshooting appendix.

For troubleshooting information about a particular Oracle Access Manager component or feature, refer to the appropriate manual in the Oracle Access Manager 10.1.4.3 documentation set. See the "Road Map to Manuals" section in the *Oracle Access Manager Introduction* manual for a description of each manual in the Oracle Access Manager documentation set.

10.6.5.1 User is Redirected to the Login Screen After Activating Some Administration Console Changes

Problem

After configuring Oracle HTTP Server and the load balancing router to access the Oracle WebLogic Administration console, some activation changes cause redirection to the login screen for the WebLogic Server Administration Console.

Solution

This is the result of the Administration Console tracking changes made to ports, channels, and security settings made using the Administration Console. For certain changes the Console may redirect the user's browser to the Administration Server's listen address. Activation is completed regardless of the redirection. It is not required to log in again; users can simply update the URL to the following and then access the Home page for the Administration Console directly:

```
admin.mycompany.com/console/console.portal
```

10.6.5.2 User is Redirected to the Administration Console's Home Page After Activating Some Changes

Problem

After configuring Oracle Access Manager, some activation changes cause redirection to the Administration Console Home page (instead of the context menu where the activation was performed).

Solution

This is expected when Oracle Access Manager single sign-on is configured and is a result of the redirections perfromed by the Administration Server. Activation is completed regardless of the redirection. If required, user should manually navigate again to the desired context menu.

10.6.5.3 OAM Configuration Tool Does Not Remove Invalid URLs

Problem

If the policy domain has an invalid or incorrect URL, running the OAM Configuration Tool with the correct URLs will not update the Policy Manager, even though the tool completes successfully.

Solution

The OAM Configuration Tool adds new URLs to an existing policy domain when run using an existing `app_domain` name. It does not remove any of the existing URLs. The Policy Manager Console must be used to remove any invalid URLs. Follow these steps to update the URLs in an existing policy domain:

1. Access the Policy Manager Console using the following URL:

   `http://`*`hostname`*`:`*`port`*`/access/oblix`

   For example, enter the following URL in your web browser:

   `http://oamadminhost.mycompany.com:7777/access/oblix`

2. When prompted, log in using the `administrator` user credentials.
3. On the landing page, click the **Policy Manager** link.
4. On the Policy Manager Console, click the **My Policy Domains** link.
5. On the My Policy Domains page, click the link for the appropriate policy domain.
6. On the Policy Domain page, select the **Resources** tab.
7. On the Resources page, select the valid or incorrect URLs and delete them.

10.7 Other Recommendations

This section describes some other recommendations for the Oracle Identity Management enterprise deployment.

10.7.1 Preventing Timeouts for SQL*Net Connections

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (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 RAC, set this parameter in all of the Oracle home directories.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

V

W