Oracle® Exalogic Elastic Cloud

Enterprise Deployment Guide for Oracle Identity and Access Management

Release EL X2-2, X3-2, X4-2, and X5-2

E53318-01

May 2015

Documentation for installers that describes how to install and configure Oracle Identity and Access Management on an Exalogic platform in an enterprise deployment.

Oracle Exalogic Elastic Cloud Enterprise Deployment Guide for Oracle Identity and Access Management
Release EL X2-2, X3-2, X4-2, and X5-2

E53318-01

Primary Author: Joe Paul (Writer), Michael Rhys (Contributing Engineer)

Contributing Author: Ellen Desmond, Peter LaQuerre

Contents

3 Introduction and Planning

4 Networking Overview

5 Configuring Exalogic Networking for a Physical Environment

6 Configuring Exalogic Networking for a Virtual Environment

7 Preparing Storage for an Enterprise Deployment

8 Creating Exalogic Virtual Servers (vServers)

9 Configuring the Servers for an Enterprise Deployment

10 Preparing the Database for an Enterprise Deployment

11 Preparing for Deployment

12 Installing and Configuring Oracle Traffic Director for an Enterprise Deployment

13 Creating a Deployment Profile

14 Deploying Identity and Access Management

15 Performing Post-Deployment Configuration

16 Validating Deployment

17 Extending the Domain to Include Oracle Adaptive Access Manager

18 Configuring Server Migration for an Enterprise Deployment

19 Scaling Enterprise Deployments

20 Managing the Topology for an Enterprise Deployment

A Automation of the Process

B Cleaning Up an Environment Before Rerunning IAM Deployment

C Topology Tool Commands for Scaling

D Configuring External Access to an Internal Exalogic IAM Deployment

List of Tables

List of Figures

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Exalogic Elastic Cloud documentation set:

- *Oracle Exalogic Elastic Cloud Administrator's Guide*
- *Oracle Exalogic Elastic Cloud Machine Owner's Guide*
- *Oracle Exalogic Elastic Cloud Multi-Rack Cabling Guide*
- *Oracle Exalogic Enterprise Deployment Guide*

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

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administrator's Guide*

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Solaris Operating System*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for HP-UX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for hp Tru64 UNIX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for AIX Based Systems*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*
- *Oracle Database Backup and Recovery User's Guide*

Conventions

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

The following text conventions are used in this document:

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

What's New in This Guide

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

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

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

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

1 Overview

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

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

This chapter contains the following sections:

- Section 1.1, "What Is an Enterprise Deployment?"
- Section 1.2, "About the Reference Topology for Exalogic"
- Section 1.3, "Benefits of Oracle Recommendations"

1.1 What Is an Enterprise Deployment?

An enterprise deployment is a carefully designed, reference topology, which demonstrates how you can install, configure, extend, and manage Oracle Fusion Middleware in a typical production environment.

A production environment is an environment where you must take into account high-availability and security considerations, so you can deploy business-critical, custom applications. The people (customers, employees, co-workers) who use your applications can access them from the Internet safely and securely.

In an enterprise deployment, you achieve high availability by deploying the Oracle Fusion Middleware products across multiple hosts. You can then use a hardware load balancer, Oracle WebLogic Server clusters, an Oracle Real Application Clusters database to allow for failover when a host is unavailable.

You build in security by setting up firewalls between the tiers of the topology to restrict access to critical software and hardware components. Security also involves integrating the enterprise deployment with Oracle Identity and Access Management products, which provide authentication, authorization, other important security features.

The enterprise deployment is not the only supported topology for an Oracle Fusion Middleware environment. However, it serves as an example (or reference) you can use to build an environment that meets the needs of your organization and your application users.

1.2 About the Reference Topology for Exalogic

This guide provides a reference topology designed specifically for Exalogic.

Wherever possible, the topology has been modified to take advantage of the unique performance capabilities of the Exalogic Infiniband network fabric. It has also been designed to take advantage of Oracle Traffic Director and ZFS Storage appliance, both of which are available on the Exalogic platform.

Before you start implementing the Oracle Exalogic enterprise deployment topology, you should understand the current state of the Exalogic environment.

For example, it is assumed that you have completed all tasks described in the *Oracle Fusion Middleware Exalogic Machine Owner's Guide*, which discusses your data center site preparation, Oracle Exalogic machine commissioning, initial networking configuration including IP address assignments, and initial setup of the Sun ZFS Storage 7320 appliance.

As with other Enterprise Deployment Guides, you should use the topologies described in this guide as an example (or reference) topology on Exalogic machine, which can be modified to meet the specific needs of your organization.

1.3 Benefits of Oracle Recommendations

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

This section contains the following topics:

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

1.3.1 Built-in Security

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

- Even if external communication is received on port 80, it is redirected to port 443
- External communication uses the Secure Socket Layer (SSL) secure Web Protocol. This is terminated at the site's load balancer.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the application or data tier is allowed.
- Direct communication across two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- All communication between components across firewalls 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 without a single point of failure.

2

Introduction to Oracle Identity and Access Management on Exalogic

This is a chapter describes Exalogic and the characteristics of an Oracle Identity and Access Management deployment on an Exalogic environment.

This chapter includes the following topics:

- Section 2.1, "Understanding Exalogic"
- Section 2.2, "Understanding Oracle Traffic Director"
- Section 2.3, "About Exalogic Optimizations for WebLogic"

2.1 Understanding Exalogic

This section provides an overview of how exalogic functions in an Oracle Identity and Access Management enterprise deployment.

- Section 2.1.1, "What is Exalogic?"
- Section 2.1.2, "Understanding Types of Deployment"

2.1.1 What is Exalogic?

Oracle Exalogic is an integrated hardware and software system designed to provide a complete platform for a wide range of application types and widely varied workloads. Exalogic is intended for large-scale, performance-sensitive, mission-critical application deployments. It combines Oracle Fusion Middleware software and industry-standard Sun hardware to enable a high degree of isolation between concurrently deployed applications, which have varied security, reliability, and performance requirements. With Exalogic, you can develop a single environment that can support end-to-end consolidation of your applications.

Exalogic includes the following components:

- Servers (compute nodes)
- Storage Area Network (SAN) (ZFS Storage Appliance)
- Integrated Networking (wires and switches)

For more information about Exalogic, see ’Introduction to Exalogic Machine’ in the *Oracle Exalogic Elastic Cloud Machine Owner’s Guide*.

2.1.1.1 About the Exalogic Hardware Architecture

This section describes the Oracle Exalogic hardware architecture.

This section contains the following topics:

- Section 2.1.1.1.1, "About Compute Nodes"
- Section 2.1.1.1.2, "About Exalogic Storage"
- Section 2.1.1.1.3, "About Exalogic Networking"
- Section 2.1.1.1.4, "Understanding Exalogic Components"

Oracle's Exalogic was tested extensively on a wide range of hardware configurations to arrive at the optimal configuration for middleware type deployments. Design considerations included high availability, compute density, state-of-the-art components, balanced system design, field serviceability, centralized storage, and high-performance networking.

2.1.1.1.1 About Compute Nodes Processing is performed by compute nodes. The compute nodes are much like servers. These compute nodes contain CPU's, Networking and internal flash storage.

A full rack of Exalogic has 30 compute nodes, a half-rack has 16 compute nodes, a quarter-rack has 8 compute nodes, and a one-eighth rack has 4 compute nodes.

The compute node resembles traditional server hardware and is designed to be a general-purpose processing unit, although its hardware and software have been specifically constructed and tuned to run Java-based middleware software.

Compute nodes are pre-loaded with the Exalogic Linux base image. They can be re-imaged with either a Solaris or OVM server. You can run any type of application you want on a compute node if it is supported on the operating system.

Compute nodes balance high performance with high density. Density is a measure of computing power within a given amount of floor space in a data center. You could have multiple applications deployed on a single compute Node. You could configure the compute Node to have a backup compute node.

Compute nodes are the physical computing resources (servers) within the Exalogic rack. Compute nodes can either be used directly as in a physical deployment or configured to host a virtual environment in the case of a virtual Exalogic deployment.

In either case the compute nodes must have the following:

- The correct packages installed
- Correct kernel parameters
- Time Server
- Storage mounted
- Up-to-date Exalogic bundle patches

For information about hardware requirements, see Section 3.6.2, "Exalogic Machine Requirements."

2.1.1.1.2 About Exalogic Storage Shared storage is provided by a Sun ZFS Storage 7320 appliance, which is accessible by all the compute nodes. ZFS storage features optimized compression, performance and reliability optimizations and is built in to the Exalogic machine. With ZFS, storage has been specifically engineered to hold the binaries and configurations for both middleware and applications therefore reducing the number of installations and simplifying configuration management on the Exalogic system.

The Exalogic storage subsystem consists of two physically separate storage heads in an active/standby configuration and large shared disk array. Each of the storage heads is directly attached to the I/O fabric with redundant QRD InfiniBand. The storage subsystem is accelerated with two types of solid state memory that are used as read and write caches, respectively, in order to increase system performance. The storage heads transparently integrate the many Serial Attached SCSI disks in the disk array into a single ZFS cluster which is then made available to Exalogic compute nodes through standard network file systems supported by the compute node's operating system.

By ensuring that all Fusion Middleware software and configuration information is stored on the ZFS appliance, you make it easier to use the ZFS integrated snapshot and remote mirroring capabilities to ensure the integrity of the configuration.

To organize the enterprise deployment software on the appliance, you create a project, and then create shares within that project so you can mount the shares to each compute node.

For more information and specific instructions for configuring Sun ZFS Storage appliance, see Section 7.5, "Configuring Exalogic Storage for Oracle Identity Management."

2.1.1.1.3 About Exalogic Networking Exalogic systems have of three network areas - Management, IP over InfiniBand (IPoIB), and Ethernet over InfiniBand (EoIB).

- **IPoIB Network** - This network is used for inter rack communication. This network is the fastest available, but cannot be accessed from outside of the Exalogic machine rack.
- **Management network** - This ethernet network allows people to connect to the individual compute nodes from the public ethernet. It is used for management and setup only. This network should not be used for regular ethernet communications.
- **EoIB Network** - You can configure this network manually to allow communication between compute nodes and the external public network. This network would be used when:
  - You wish the external load balancer to communicate with the Oracle traffic Director instances installed within the Exalogic rack on compute nodes or vServers.
  - You wish your compute nodes/virtual servers to communicate with an external database.
  - You wish external Web servers (Oracle HTTP servers) to communicate with the WebLogic managed servers running on the compute nodes/virtual servers.

InfiniBand and Ethernet switches enable network communication in Exalogic. InfiniBand provides reliable delivery, security and quality of service at the physical layer in the networking stack, with a maximum bandwidth of 40Gb/s and latency down to 1 millisecond. The compute and storage nodes include InfiniBand network adapters, which are also referred to as host channel adapters (HCAs). The dual-port infiniband HCA provides a private internal network connecting the compute nodes and storage nodes to the system's I/O fabric.

The operating system images shipped with Exalogic are bundled with a suite of infiniBand drivers and utilities called OpenFabrics Enterprise Distribution (OFED). Oracle Fusion Middleware software contains optimizations that leverage OFED to provide higher performance over infiniband

IB networking is used for all communications and data transfers within the Exalogic machine and can be used to connect multiple Oracle Engineered Systems together to create a very high performance, multi-purpose computing environment.

Although the hardware within Exalogic utilizes an InfiniBand fabric, the rest of your data center, along with the outside world, still speaks only Ethernet. This includes your application clients, such as web browsers, as well as legacy enterprise information systems, which components running within Exalogic may need to communicate with. Exalogic's switches and nodes enable this communication through the Ethernet over InfiniBand (EoIB) protocol. As the name suggests, EoIB gives InfiniBand devices the ability to emulate an Ethernet connection using IB hardware.

2.1.1.1.4 Understanding Exalogic Components Oracle Exalogic is delivered as a Rack of hardware which consist of the following components

Exalogic includes the following components:

- Servers (compute nodes)
- Storage Area Network (SAN) (ZFS Storage Appliance)
- Integrated Networking (wires and switches)

In addition to the hardware components, Exalogic comprises Oracle Exalogic Elastic Cloud software, which consists of pre-integrated, standard technologies including the operating system, virtualization technology, networking software, device drivers, and firmware.

For more information about Exalogic, see 'Introduction to Exalogic Machine' in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

2.1.2 Understanding Types of Deployment

This section describes the types of Exalogic deployment.

This section includes the following topics:

- Section 2.1.2.1, "About a Physical Exalogic Configuration"
- Section 2.1.2.2, "About a Virtual Exalogic Configuration"
- Section 2.1.2.3, "About Choosing a Type of Deployment"

2.1.2.1 About a Physical Exalogic Configuration

In a physical Exalogic configuration, the application software is deployed on compute nodes. Each compute node runs its own single operating system. All applications, including WebLogic Server, Coherence, and Tuxedo, then share this OS kernel and the local compute node resources.

The Exalogic compute nodes are engineered servers and thus provide extreme performance to Java-based Middleware software deployed on the compute nodes.

This configuration does not include Oracle VM and middleware. In addition, applications running on the Exalogic platform are deployed and managed in very much the same way as they are on traditional platforms; new deployments are associated with appropriate physical compute, storage, memory and I/O resources. Enterprise Manager is the primary administration tool.

2.1.2.2 About a Virtual Exalogic Configuration

The purpose of server virtualization is to fundamentally isolate the operating system and applications stack from the constraints and boundaries of the underlying physical servers. By doing this, multiple virtual machines can be presented with the impression that they are each running on their own physical hardware when, in fact, they are sharing a physical server with other virtual machines. This allows server consolidation in order to maximize the utilization of server hardware, while minimizing costs associated with the proliferation of physical servers-namely hardware, cooling, and real estate expenses.

This hardware isolation is accomplished either through a software based sharing or a direct device assignment (where a I/O device is directly assigned to a VM). Software based sharing is achieved by inserting a very thin layer of software between the OS in the virtual machine and the underlying hardware to either directly emulate the hardware or to otherwise manage the flow and control of everything from CPU scheduling across the multiple VMs, to I/O management, to error handling.

The challenge with Virtualization is to achieve a high enough consolidation ratio to achieve the cost benefits you need while still being able to provide the exceptional, predictable performance required from your core applications.

2.1.2.2.1 About the Oracle Exalogic Elastic Cloud In the latest version of Oracle Exalogic, Oracle has virtualized the InfiniBand connectivity in Exabus, using state-of-the-art, standards-based technology to permit the consolidation of multiple virtual machines per physical server with no impact on performance. This is known as the Oracle Exalogic Elastic Cloud. Converting an Exalogic rack to an Oracle Exalogic Elastic cloud rack is optional and involves commissioning the Exalogic rack with the Oracle Exalogic Elastic cloud software.

Oracle Exalogic Elastic Cloud includes support for a highly optimized version of the Oracle VM Hypervisor, which can be used to subdivide a physical compute node into multiple virtual servers (vServers), each of which may run a separate Oracle Linux operating system instance and applications.

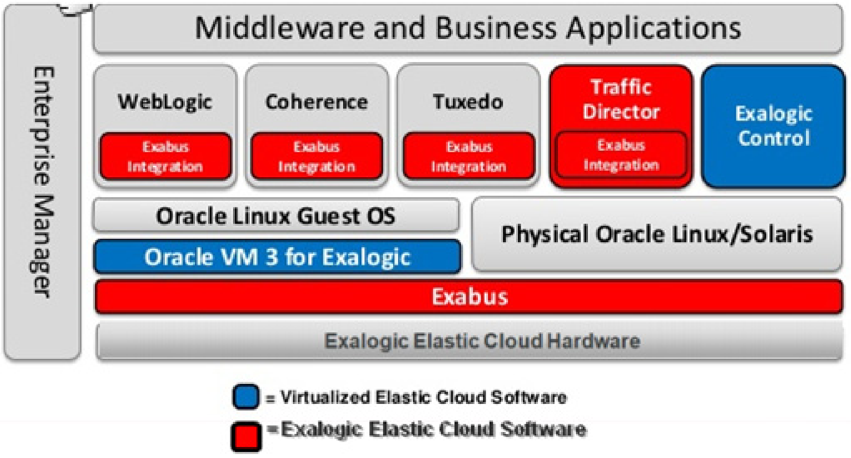
Oracle VM for Exalogic uses a technology called Single Root I/O Virtualization (SRIOV), which has been designed in a manner to eliminate virtualization overhead such as to provide maximum performance and scalability.

The logical vServers can have specific amounts of physical compute, storage, memory and I/O resources, optionally pre-configured with middleware and applications. This approach allows for maximum levels of resource sharing and agility as vServers can share physical resources and can be provisioned in minutes. Pre-configured OVM templates for Oracle Applications are available to download.

Oracle Elastic Cloud Architecture

Oracle Exalogic Elastic Cloud is Oracle's first engineered system for enterprise Java.

Figure 2–1 Oracle Exalogic Elastic Cloud



Oracle has made unique optimizations and enhancements to Exalogic components, as well as Oracle's Fusion middleware and Oracles applications, which includes on-chip network virtualization, high performance Remote Direct Memory Access (RDMA) at operating system and Java Virtual Machine (JVM) layers and Exalogic-aware workload management in Oracle Weblogic server (Oracle's Java EE application server), to meet the highest standards of reliability, availability, scalability and performance.

Exalogic Elastic Cloud comprises Exabus, which is a set of hardware, firmware and software optimizations that enable the operating system, middleware components and even certain Oracle applications to make full use of the infiniband fabric and the Oracle Traffic Director.

The InfiniBand network fabric, as we discussed in previous section, offers extremely high bandwidth and low latency, which provides major performance gains with respect to communication between the application server and the database server, and with respect to communication between different application server instances running with in the Exalogic system.

The current release of the Exalogic Elastic Cloud Software includes a tightly integrated server virtualization layer with unique capabilities allowing the consolidation of multiple, separate virtual machines containing applications or Middleware on each server node while introducing essentially no I/O virtualization overhead to the Exabus InfiniBand network and storage fabric.

Physically, Oracle Exalogic Elastic Cloud can be viewed as a rack of physical server machines plus centralized storage, which all have been designed together to cater to typical high-performance Java application use cases.

Understanding Exalogic Elastic Cloud Architecture

The Exalogic system consists of the following two major elements:

- Exalogic X4-2 - A high performance hardware system, assembled by Oracle that integrates storage and compute resources using a high-performance I/O subsystem called Exabus, which is built on Oracle's Quad Data Rate (QDR) InfiniBand.
- Exalogic Elastic Cloud Software - An essential package of Exalogic-specific software, device drivers and firmware that is pre-integrated with Oracle Linux and Solaris, enabling Exalogic's advanced performance and Infrastructure-as-a-Service (IaaS) capability, server and network virtualization, storage and cloud management capabilities.

Figure 2–1 shows the Middleware software that is part of the Elastic Cloud and contains Exalogic specific optimizations. Exalogic specific optimizations in some of the Oracle Fusion Middleware applications have been described below.

- WebLogic Server - Session replication uses the SDP layer of IB networking to maximize performance of large scale data operations as this avoids some of the typical TCP/IP network processing overhead. When processing HTTP requests, WLS makes native use of the SDP protocol when called by the Oracle Traffic Director, or when making HTTP requests to it. Through its Active Gridlink for RAC feature, WLS JDBC connections and connection pools can be configured to use the low level SDP protocol when communicating natively with Exadata over the IB fabric.
- Coherence - Cluster communication has been dramatically redesigned to further minimize network latency when processing data sets across caches. Its elastic data feature increases performance in conjunction with the compute nodes built in solid state drives by optimizing both the use of RAM and garbage collection processing to minimize network and memory use. When sending data between caches it uses only an RDMA level IB verb set, thus avoiding nearly all the TCP/IP network processing overhead.
- Tuxedo - Tuxedo has been similarly enhanced to make increasing use of SDP and RDMA protocols in order to optimize the performance of inter-process communications within and between compute nodes.

2.1.2.3 About Choosing a Type of Deployment

Both of these Exalogic implementation styles can support the creation of a private cloud. In a virtualized system, Exalogic Control is used to define, manage and monitor cloud users and services. In a physical system, equivalent functionality is provided by Enterprise Manager with the Cloud Management Pack.

Among the benefits of using virtualized approach is application consolidation, tenant isolation (provision secure Exalogic resources to multiple tenants), deployment simplification, including scaling up or down. With the advent of Exalogic Elastic Cloud technology, the impact of virtualization on application throughput and latency has been minimized to negligible. Applications running in Exalogic vServers perform on par with deployments on bare metal, but retain all of the manageability and efficiency benefits that come with server virtualization.

2.2 Understanding Oracle Traffic Director

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

For information about installing and configuring Oracle Traffic Director, see Chapter 12, "Installing and Configuring Oracle Traffic Director for an Enterprise Deployment."

This section contains the following topics

- Section 2.2.1, "About Oracle Traffic Director in a Standard Exalogic Deployment."
- Section 2.2.2, "About Oracle Traffic Director in a Deployment with Oracle HTTP Server."
- Section 2.2.3, "About Oracle Traffic Director Failover Groups."
- Section 2.2.4, "About Oracle Traffic Director and the Load Balancer."

- Section 2.2.5, "About Oracle Traffic Director and Identity and Access Management."

2.2.1 About Oracle Traffic Director in a Standard Exalogic Deployment

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

- LDAP
- Internal call backs

Oracle Traffic Director also proxies Web requests to WebLogic Servers. It receives requests from the load balancer on the EoIB network, and sends requests to WebLogic servers and to Oracle Unified Directory using the IPoIB network.

For more information about the standard Exalogic topology described in this guide, see Section 3.2.1, "Primary Topologies."

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

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

- LDAP
- Internal call backs

Oracle Traffic Director sends requests to Oracle HTTP Server (OHS), which resides on commodity servers on the corporate ethernet network. WebLogic servers and to Oracle Unified Directory using the IPoIB network. OHS sends requests to WebLogic Servers using the EoIB network.

For more information about using Oracle HTTP Server as a Web tier instead of Oracle Traffic Director, see Section 3.2.2.1, "Using an External Oracle HTTP Server Web Tier Instead of Oracle Traffic Director."

2.2.3 About Oracle Traffic Director Failover Groups

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

For information about creating and configuring failover groups, see Section 12.12, "Creating a Failover Group for Virtual Hosts."

2.2.4 About Oracle Traffic Director and the Load Balancer

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

2.2.5 About Oracle Traffic Director and Identity and Access Management

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

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

2.3 About Exalogic Optimizations for WebLogic

Oracle Exalogic includes performance optimizations for Oracle WebLogic Server to improve input/output, thread management, and request handling efficiency. You can configure a WebLogic Server domain to enable domain-wide input/output optimizations. These optimizations include multi-core architectural enhancements that improve thread management, request processing, and reduce lock contention.

Additional optimizations include reduced buffer copies, which result in more efficient input/output. Finally, session replication performance and CPU utilization is improved through lazy de-serialization, which avoids performing extra work on every session update that is only necessary when a server fails.

You can configure WebLogic Server clusters with cluster-wide optimizations that further improve server-to-server communication. The first optimization enables multiple replication channels, which improve network throughput among WebLogic Server cluster nodes. The second cluster optimization enables InfiniBand support for Sockets Direct Protocol, which reduces CPU utilization as network traffic bypasses the TCP stack.

For more information about, and procedures for Exalogic Optimization see Section 15.7, "Enabling Exalogic Optimizations."

3 Introduction and Planning

This chapter describes and illustrates the enterprise deployment reference topology described in this guide and helps you plan your deployment.

This chapter contains the following topics:

- Section 3.1, "Planning Your Deployment"
- Section 3.2, "Understanding the Oracle Identity Management Deployment Topology on Exalogic"
- Section 3.3, "Understanding the Topology Components"
- Section 3.4, "About Oracle Directory Services Manager"
- Section 3.5, "Benefits of Using the Split Domain Topology"
- Section 3.6, "Hardware Requirements for the Identity Management on Exalogic"
- Section 3.7, "Software Components for an Enterprise Deployment"
- Section 3.8, "Road Map for the Reference Topology Installation and Configuration"

3.1 Planning Your Deployment

This section provides information to help you plan the deployment of Oracle Identity Management on Exalogic:

- Section 3.1.1, "Why the Deployment Topology in This Guide?"
- Section 3.1.2, "Using a Worksheet to Plan for the Deployment Topology"

3.1.1 Why the Deployment Topology in This Guide?

When planning your deployment, you should be aware that this guide provides detailed instructions for implementing the specific reference topology described in this chapter.

This topology takes advantage of key features of the Exalogic platform, including:

- The high bandwidth and performance of the Exalogic internal Infiniband (IPoIB) network fabric
- The software load balancing capabilities of Oracle Traffic Director.

In this specific topology, Oracle Traffic Director is used as both a Web Listener and as a client-side load balancer for internal communication.

By using this configuration, you can take advantage of the Exalogic default IPoIB network for all internal communications between the Traffic Director instances and the Identity and Access Management compute nodes.

Only external traffic between the Traffic Director instances and external users is on the Exalogic Ethernet over IB (EoIB) network.

3.1.2 Using a Worksheet to Plan for the Deployment Topology

The key to a successful Enterprise Deployment is planning and preparation. The road map for installation and configuration in this chapter directs you to the appropriate chapters for the tasks you need to perform.

Use this chapter to help you plan your Oracle Identity and Access Management enterprise deployment on an Exalogic platform.

You can also use the worksheets in Section 11.1, "Assembling Information for Identity and Access Management Deployment" to help you keep track of information, such as host names, IP addresses, and other important information as you procure and identify the machines and resources required for this deployment.

3.2 Understanding the Oracle Identity Management Deployment Topology on Exalogic

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

The following information applies to all the topologies described in this guide.

- Users submit requests to Oracle Identity Management from their client browsers. Each request originates as an SSL request, ensuring that the request is encrypted. The request is routed to a load balancer in the corporate DMZ.
- Upon receiving the request the Load Balancer decrypts the encrypted request and then passes this on to WEBHOST1 or WEBHOST2 using a non encrypted transaction.
- Traffic leaving the organization to go back to the client is encrypted into SSL by the load balancer.
- Terminating SSL at the load balancer ensures that optimum performance is achieved due to the fact that SSL traffic is processed entirely by the load balancer.
- A firewall exists between the DMZ and the Exalogic host to ensure that only valid traffic can enter and leave the Application Zone. Additionally a second firewall exists partitioning the network from the Application Tier to the Data Tier to ensure that only valid traffic is allowed to pass from the application tier to the database tier.
- Each of the deployment topologies is divided into 3 Zones.
  - The Demilitarized Zone (DMZ) which is accessible from the public internet. This is the entry point to the organization for client requests.
  - The Application Tier which is only accessible via the DMZ. Client traffic does not have direct access to the Application Tier.

  - The Data Tier which is only accessible via the application tier. Client traffic does not have direct access to the data tier.

  By compartmentalizing the topology in this way, you prevent unauthorized traffic from gaining access to a zone to which it is not entitled.

- The load balancer is used in conjunction with DNS to ensure that applications are only available to those that need it. The entry point sso.mycompany.com is available in the public dns and as such everyone has access to it as this is where authentication takes place.
- The urls IADADMIN.mycompany.com and IGDADMIN.mycompany.com are used to direct traffic to the administrative consoles within the application. These names are only resolvable in the corporate DNS. This ensures that external clients trying to access administrative resources cannot do so because the URLs are non resolvable. Only traffic originating inside the corporate network will be able to access these administrative functions thereby adding another layer of security to the system.

This section contains the following topics:

- Section 3.2.1, "Primary Topologies"
- Section 3.2.2, "Alternative Deployment Topologies"

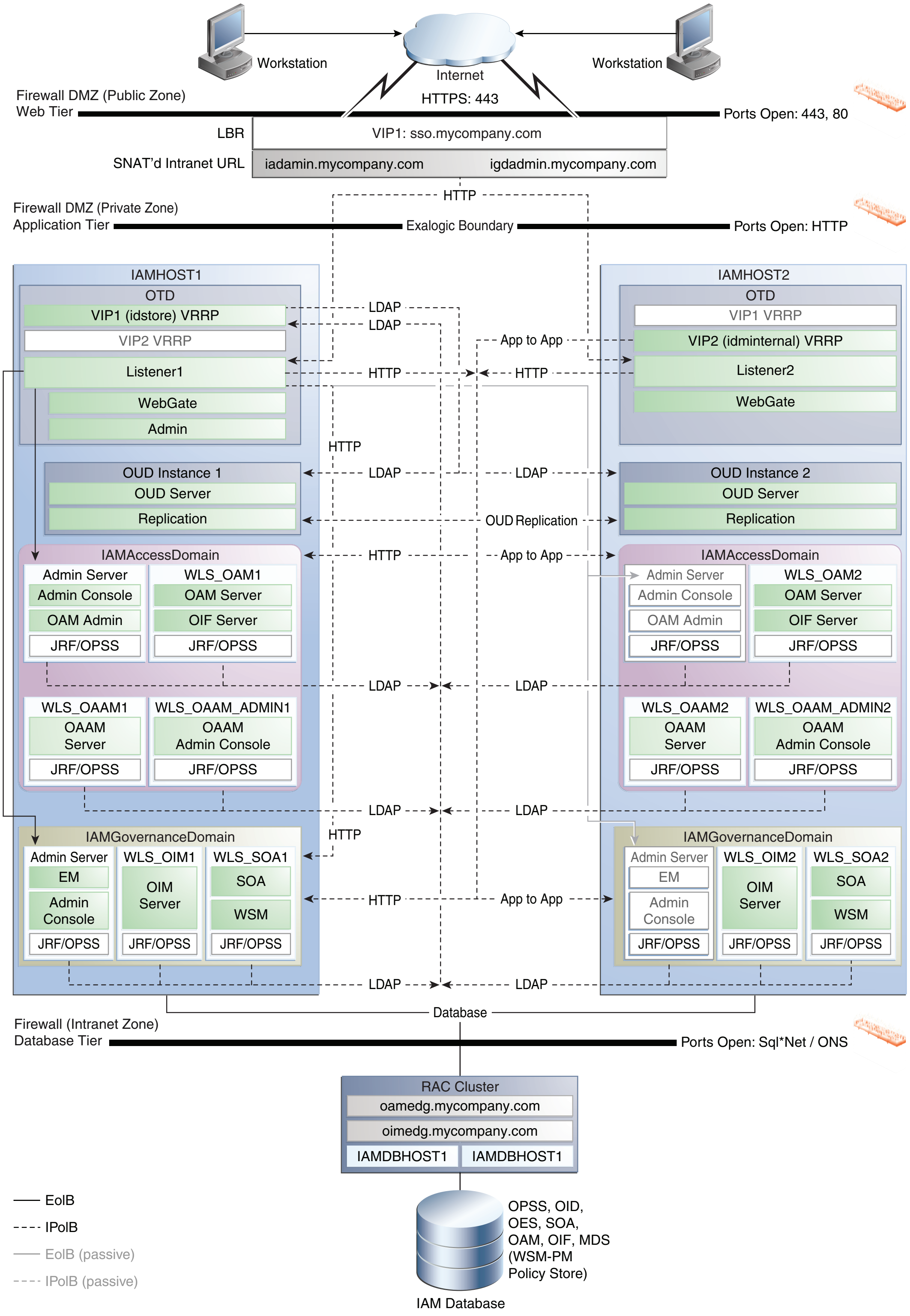
3.2.1 Primary Topologies

This guide shows two main deployment models. The first uses a physical Exalogic deployment, which is an Exalogic Rack which is used in its native form. In a physical Exalogic deployment, the compute nodes are so powerful that the entire Identity and Access Management suite can be deployed onto a single compute node, with a second compute node being used to provide high availability.

The second topology described in the guide describes where the Exalogic Rack has been virtualized using the Exalogic Elastic Cloud software. In this environment, instead of using the physical compute nodes directly, virtual servers are created and run on a number of compute nodes within the rack. For this type of deployment, the Identity and Access Management components are distributed across a number of virtual servers (vServers).

3.2.1.1 Physical Exalogic Deployment Topology

Figure 3–1 Exalogic Physical Deployment Topology


Workstation
Internet
Workstation
HTTPS: 443
Firewall DMZ (Public Zone)
Web Tier
Ports Open: 443, 80
LBR
VIP1: sso.mycompany.com
SNAT'd Intranet URL
iadmin.mycompany.com
igdadmin.mycompany.com
HTTP
Firewall DMZ (Private Zone)
Application Tier
Exalogic Boundary
Ports Open: HTTP
IAMHOST1
OTD
VIP1 (idstore) VRRP
VIP2 VRRP
Listener1
WebGate
Admin
IAMHOST2
OTD
VIP1 VRRP
VIP2 (idminternal) VRRP
Listener2
WebGate
LDAP
LDAP
App to App
HTTP
HTTP
HTTP
OUD Instance 1
OUD Server
Replication
OUD Instance 2
OUD Server
Replication
LDAP
LDAP
OUD Replication
HTTP
App to App
IAMAccessDomain
Admin Server
Admin Console
OAM Admin
JRF/OPSS
WLS_OAM1
OAM Server
OIF Server
JRF/OPSS
IAMAccessDomain
Admin Server
Admin Console
OAM Admin
JRF/OPSS
WLS_OAM2
OAM Server
OIF Server
JRF/OPSS
LDAP
LDAP
WLS_OAAM1
OAAM Server
JRF/OPSS
WLS_OAAM_ADMIN1
OAAM Admin Console
JRF/OPSS
WLS_OAAM2
OAAM Server
JRF/OPSS
WLS_OAAM_ADMIN2
OAAM Admin Console
JRF/OPSS
LDAP
LDAP
HTTP
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Server
JRF/OPSS
WLS_SOA1
SOA
WSM
JRF/OPSS
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Server
JRF/OPSS
WLS_SOA2
SOA
WSM
JRF/OPSS
HTTP
App to App
LDAP
LDAP
Database
Firewall (Intranet Zone)
Database Tier
Ports Open: Sql*Net / ONS
RAC Cluster
oamedg.mycompany.com
oimedg.mycompany.com
IAMDBHOST1
IAMDBHOST1
OPSS, OID,
OES, SOA,
OAM, OIF, MDS
(WSM-PM
Policy Store)
IAM Database
EoIB
IPoIB
EoIB (passive)
IPoIB (passive)

This figure is a graphical representation of the Physical Exalogic Deployment topology. It includes icons and symbols that represent the hardware load balancer, compute nodes, firewalls, and other elements of the topology.

At a high level, it shows the main components of the topology, including the following:

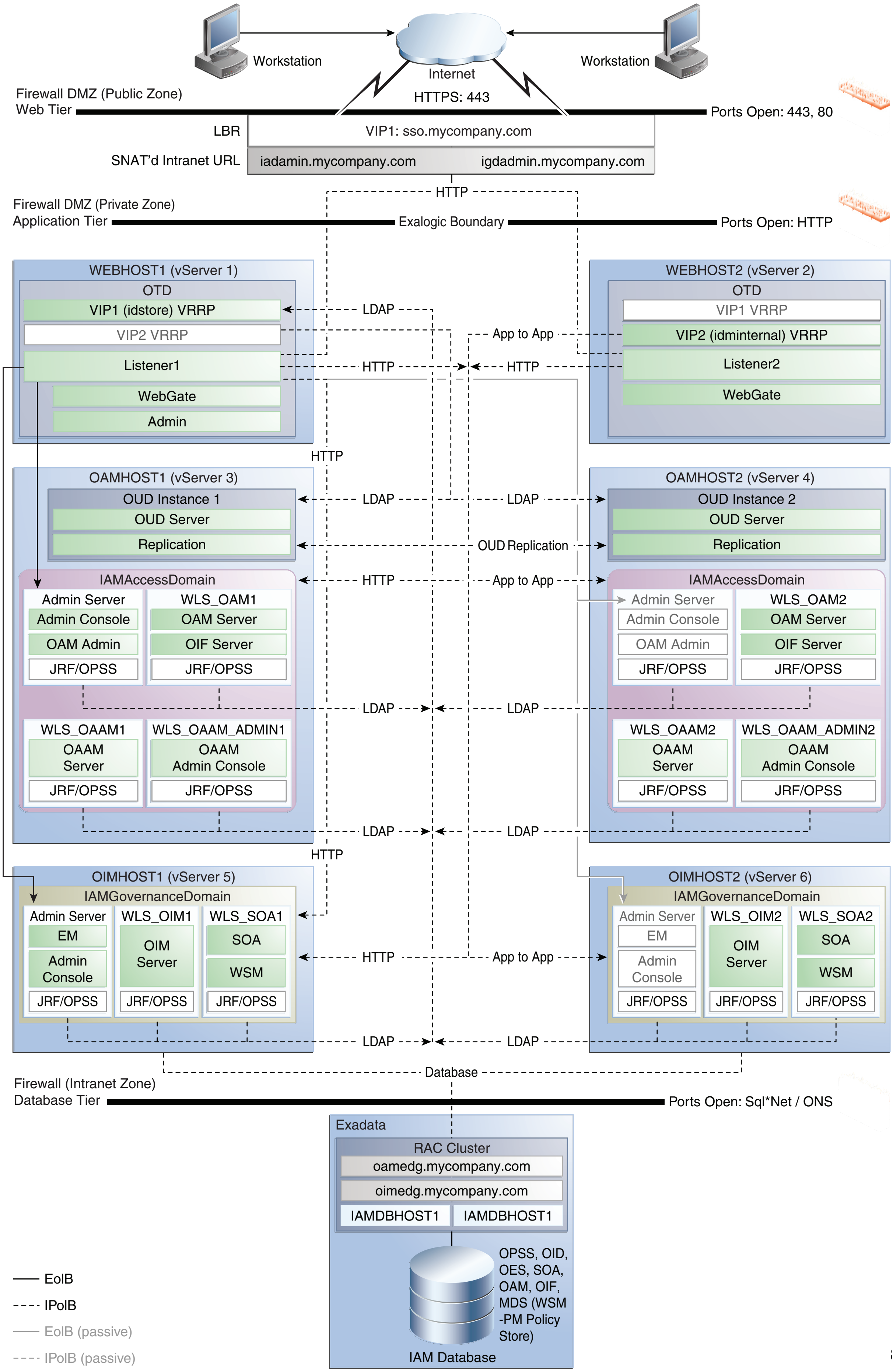
- The Web Tier, which contains a hardware load balancer which receives requests on SSO.mycompany.com, IADADMIN.mycompany.com and IGDADMIN.com and forwards them on to the Oracle Traffic Director instances on IAMHOST1 and IAMHOST2. In the case of SSO.mycompany.com, requests are SSL encrypted. SSO.mycompany.com handles requests using the HTTP protocol.
- The Application Tier, where the application servers reside, including Oracle WebLogic Server and the upper stack products, such as Oracle SOA Suite. In this specific topology, the compute nodes are referred to as IAMHOST1 and IAMHOST2.
  - Oracle Traffic Director. This topology uses Oracle Traffic director as both a web server and an internal load balancer.
  - Oracle Unified Directory. Each host has an instance of Oracle Unified Directory which is used as the LDAP directory for identity information. Each Oracle Unified Directory instance is kept up to date through Oracle Unified Directory replication.
  - WebLogic Domain: IAMAccessDomain, which consists of:
    - Oracle Access Management, which hosts Access Server/Federation Server and corresponding JRF/OPSS processes.
    - Optional Oracle Adaptive Access Manager
    - WebLogic Administration Server, which hosts the WebLogic Console for IAMAccessDomain, Oracle Enterprise Manager Fusion Middleware Control, and Access Management Console. In the event of the failure of IAMHOST1, the WebLogic Administration Server can be started on IAMHOST2.
  - WebLogic Domain: IAMGovernanceDomain, which consists of:
    - Oracle Identity Manager, which hosts an OIM Server and corresponding JRF/OPSS processes
    - SOA, which hosts a SOA Server and corresponding JRF/OPSS processes
    - WebLogic Administration Server, which hosts the Oracle WebLogic Console for IAMGovernanceDomain, Oracle Enterprise Manager Fusion Middleware Control, and Authorization Policy Manager (APM). In the event of the failure of IAMHOST1, the WebLogic Administration Server can be started on IAMHOST2.
- The Data Tier is where the databases reside. The database tier can either be on external database servers or an attached Exadata Appliance.The databases contain customer data and the schemas required by the application tier products.
- Firewalls are used to separate the Web, Application, and Directory tiers into different zones.

Note: If an ExaLogic machine is hard wired to an Exadata machine then there is no need for a firewall restricting traffic between the Application and data tiers. All traffic is kept to the internal IPoIB network.

For more information, refer to the descriptions of the topology tiers in the sections that follow the diagrams. The instructions in this guide describe how to install and configure the software for this topology.

3.2.1.2 Virtual Exalogic Deployment Topology

Figure 3–2 Exalogic Virtual Deployment Topology


Workstation
Internet
Workstation
HTTPS: 443
Firewall DMZ (Public Zone)
Web Tier
Ports Open: 443, 80
LBR
VIP1: sso.mycompany.com
SNAT'd Intranet URL
iadamin.mycompany.com
igdadmin.mycompany.com
HTTP
Firewall DMZ (Private Zone)
Application Tier
Exalogic Boundary
Ports Open: HTTP
WEBHOST1 (vServer 1)
OTD
VIP1 (idstore) VRRP
VIP2 VRRP
Listener1
WebGate
Admin
WEBHOST2 (vServer 2)
OTD
VIP1 VRRP
VIP2 (idminternal) VRRP
Listener2
WebGate
LDAP
App to App
HTTP
HTTP
HTTP
OAMHOST1 (vServer 3)
OUD Instance 1
OUD Server
Replication
LDAP
LDAP
OUD Replication
OAMHOST2 (vServer 4)
OUD Instance 2
OUD Server
Replication
IAMAccessDomain
Admin Server
Admin Console
OAM Admin
JRF/OPSS
WLS_OAM1
OAM Server
OIF Server
JRF/OPSS
HTTP
App to App
IAMAccessDomain
Admin Server
Admin Console
OAM Admin
JRF/OPSS
WLS_OAM2
OAM Server
OIF Server
JRF/OPSS
LDAP
LDAP
WLS_OAAM1
OAAM Server
JRF/OPSS
WLS_OAAM_ADMIN1
OAAM Admin Console
JRF/OPSS
WLS_OAAM2
OAAM Server
JRF/OPSS
WLS_OAAM_ADMIN2
OAAM Admin Console
JRF/OPSS
LDAP
LDAP
HTTP
OIMHOST1 (vServer 5)
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM1
OIM Server
JRF/OPSS
WLS_SOA1
SOA
WSM
JRF/OPSS
HTTP
App to App
OIMHOST2 (vServer 6)
IAMGovernanceDomain
Admin Server
EM
Admin Console
JRF/OPSS
WLS_OIM2
OIM Server
JRF/OPSS
WLS_SOA2
SOA
WSM
JRF/OPSS
LDAP
LDAP
Database
Firewall (Intranet Zone)
Database Tier
Ports Open: Sql*Net / ONS
Exadata
RAC Cluster
oamedg.mycompany.com
oimedg.mycompany.com
IAMDBHOST1
IAMDBHOST1
OPSS, OID, OES, SOA, OAM, OIF, MDS (WSM -PM Policy Store)
IAM Database
EoIB
IPoIB
EoIB (passive)
IPoIB (passive)

This figure is a graphical representation of the Virtual Exalogic Deployment topology. It includes icons and symbols that represent the hardware load balancer, vServers, firewalls, and other elements of the topology. At a high level, it shows the main components of the topology, including the following:

- The Web Tier, which contains a hardware load balancer which receives requests on SSO.mycompany.com, IADADMIN.mycompany.com and IGDADMIN.com and forwards them on to the Oracle Traffic Director instances on WEBHOST1 and WEBHOST2.

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

- The Application Tier, where the application servers reside, including Oracle WebLogic Server and the upper stack products, such as Oracle SOA Suite. In this specific topology, there are six vServers, referred to as WEBHOST1, WEBHOST2, OAMHOST1, OAMHOST2, OIMHOST1, and OIMHOST2.

  - Oracle Traffic Director. This topology uses Oracle Traffic Director as both a web server and an internal load balancer. The Oracle Traffic Director instances reside on WEBHOST1 and WEBHOST2.

  - Oracle Unified Directory. Each host has an instance of Oracle Unified Directory which is used as the LDAP directory for identity information. Each Oracle Unified Directory instance is kept up to date through Oracle Unified Directory replication. the Oracle Unified Directory instances reside on OAMHOST1 and OAMHOST2.

  - WebLogic Domain: IAMAccessDomain, which consists of:

    - Oracle Access Management, which hosts Access Server/Federation Server and corresponding JRF/OPSS processes.

    - Optional Oracle Adaptive Access Manager

    - WebLogic Administration Server, which hosts the WebLogic Console for IAMAccessDomain, OAM Console, and Oracle Enterprise Manager Fusion Middleware Control.

    The IAMAccessDomain servers reside on OAMHOST1 and OAMHOST2. In the event of the failure of OAMHOST1, the WebLogic Administration Server can be started on OAMHOST2.

  - WebLogic Domain: IAMGovernanceDomain, which consists of:

    - Oracle Identity Manager, which hosts an OIM Server and corresponding JRF/OPSS processes

    - SOA, which hosts a SOA Server and corresponding JRF/OPSS processes

    - WebLogic Administration Server, which hosts the WebLogic Console for IAMGovernanceDomain, Oracle Enterprise Manager Fusion Middleware Control, and Authorization Policy Manager (APM).

    The IAMGovernanceDomain servers reside on OIMHOST1 and OIMHOST2. In the event of the failure of OIMHOST1, the WebLogic Administration Server can be started on OIMHOST2.

- The Data Tier is where the databases reside. The database tier can either be on external database servers or an attached Exadata Appliance.The databases contain customer data and the schemas required by the application tier products.
- Firewalls are used to separate the Web, Application, and Directory tiers into different zones.

> **Note:** If an ExaLogic machine is hard wired to an Exadata machine then there is no need for a firewall restricting traffic between the Application and data tiers. All traffic is kept to the internal IPoIB network.

For more information, refer to the descriptions of the topology tiers in the sections that follow the diagrams. The instructions in this guide describe how to install and configure the software for this topology.

3.2.2 Alternative Deployment Topologies

Besides the topologies discussed in this guide, you can consider alternative Oracle Identity Manager topologies on Exalogic.

This guide does not provide specific instructions for implementing these alternative topologies, but consider the following when you are preparing your environment for an Oracle Identity Manager deployment on Exalogic:

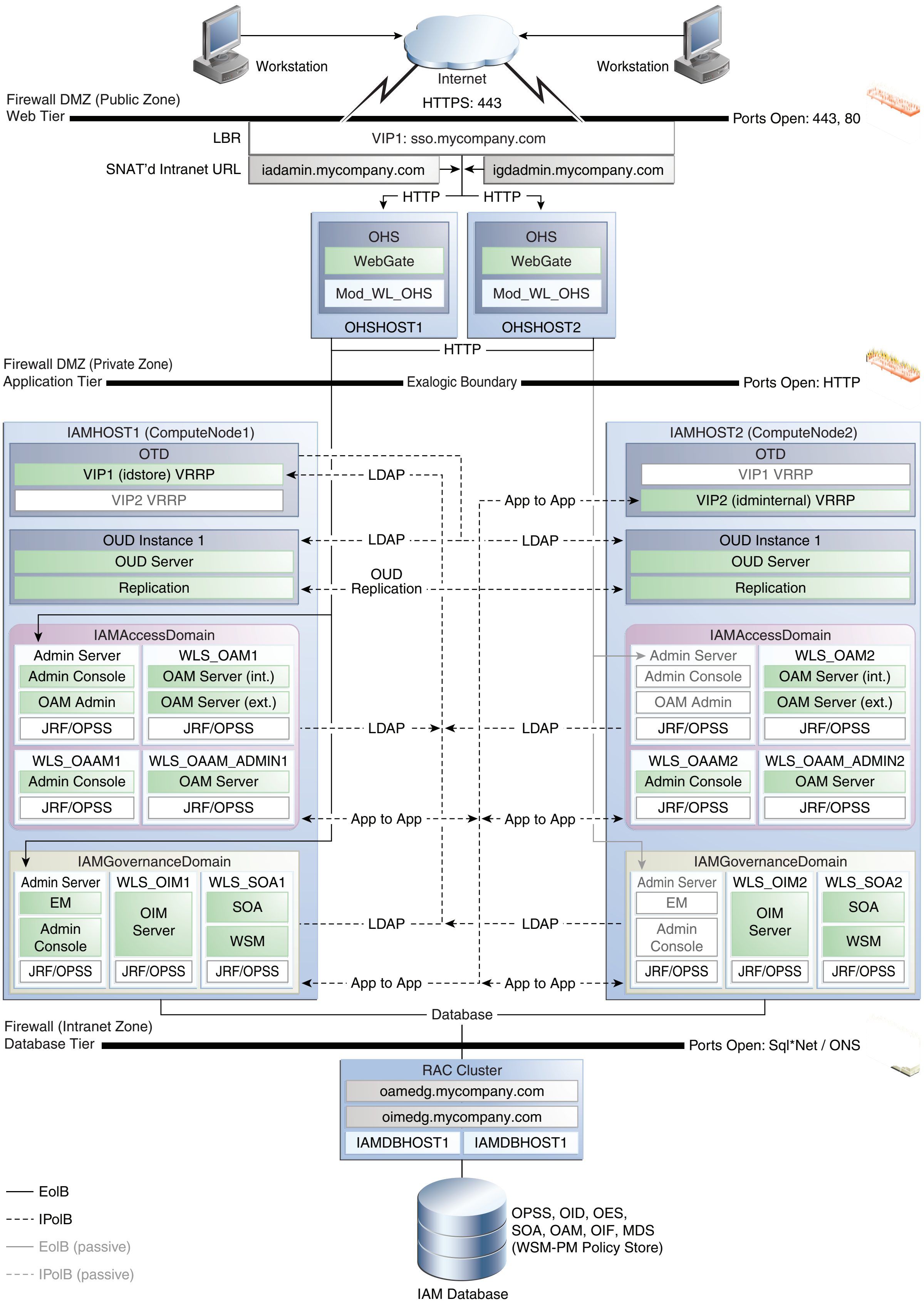
- Using an External Oracle HTTP Server Web Tier Instead of Oracle Traffic Director
- Using Oracle Exadata Instead of an Oracle RAC Database

3.2.2.1 Using an External Oracle HTTP Server Web Tier Instead of Oracle Traffic Director

The other topologies described in this guide use Oracle Traffic Director as both a Web server and an internal load balancer. You may want to, as shown in Figure 3–3, "Exalogic OHS Topology" move the external Web requests outside of the Exalogic rack into a dedicated Demilitarized Zone (DMZ). The benefit of this approach is that the new Web Hosts can be separated from the Exalogic rack using a firewall.

If you cannot dedicate two compute nodes for Oracle Traffic Director, or if you would rather use a dedicated Oracle HTTP Server Web Tier, then it is possible to deploy Oracle HTTP Server on an external Web tier, which is located outside the Exalogic machine.

Figure 3–3 Exalogic OHS Topology



This figure is a graphical representation of the Exalogic OHS Deployment topology. It includes icons and symbols that represent the hardware load balancer, compute nodes, firewalls, and other elements of the topology. At a high level, it shows the main components of the topology, including the following:

- There are two servers, Webhost1 and Webhost2, each of which hosts an Oracle HTTP Server and Oracle WebGate.

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

- The Application Tier, where the application servers reside, including Oracle WebLogic Server and the upper stack products, such as Oracle SOA Suite. In this specific topology, the compute nodes are referred to as IAMHOST1 and IAMHOST2.

  - Oracle Traffic Director. This topology uses Oracle Traffic director only as an internal load balancer.
  - Oracle Unified Directory. Each host has an instance of Oracle Unified Directory which is used as the LDAP directory for identity information. Each Oracle Unified Directory instance is kept up to date through Oracle Unified Directory replication.
  - WebLogic Domain: IAMAccessDomain, which consists of:
    - Oracle Access Management, which hosts Access Server/Federation Server and corresponding JRF/OPSS processes.
    - Optional Oracle Adaptive Access Manager
    - WebLogic Administration Server, which hosts the WebLogic Console for IAMAccessDomain, OAM Console, and Oracle Enterprise Manager Fusion Middleware Control. In the event of the failure of IAMHOST1, the WebLogic Administration Server can be started on IAMHOST2.
  - WebLogic Domain: IAMGovernanceDomain, which consists of:
    - Oracle Identity Manager, which hosts an OIM Server and corresponding JRF/OPSS processes
    - SOA, which hosts a SOA Server and corresponding JRF/OPSS processes
    - WebLogic Administration Server, which hosts the WebLogic Console for IAMGovernanceDomain, Oracle Enterprise Manager Fusion Middleware Control, and Authorization Policy Manager (APM). In the event of the failure of IAMHOST1, the WebLogic Administration Server can be started on IAMHOST2.

- The Data Tier is where the databases reside. The database tier can either be on external database servers or an attached Exadata Appliance.The databases contain customer data and the schemas required by the application tier products.

- Firewalls are used to separate the Web, Application, and Directory tiers into different zones.

> **Note:** If an ExaLogic machine is hard wired to an Exadata machine then there is no need for a firewall restricting traffic between the Application and data tiers. All traffic is kept to the internal IPoIB network.

For more information, refer to the descriptions of the topology tiers in the sections that follow the diagrams. The instructions in this guide describe how to install and configure the software for this topology.

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

3.2.2.2 Using Oracle Exadata Instead of an Oracle RAC Database

The reference topology in this guide provides information on using an external Real Application Clusters (RAC) database as the repository for product schemas and security stores.

The topology assumes that the RAC database is hosted on dedicated servers. These servers can either be independent or as part of an Oracle Exadata database machine.

If an Oracle Exadata machine is used then this should be connected to the Exalogic machine via the InfiniBand fabric. For more information, see "Connecting Exalogic and Exadata Machines" in the *Oracle Exalogic Elastic Cloud Multi-Rack Cabling Guide*.

3.3 Understanding the Topology Components

The topologies consist of three tiers, which are described in the following sections:

- Section 3.3.1, "About Exalogic Physical and Virtual Deployment Topologies"
- Section 3.3.2, "About EoIB and IPoIB Communication"
- Section 3.3.3, "About the Hardware Load Balancer"
- Section 3.3.4, "About the DMZ"
- Section 3.3.5, "About the Web Tier"
- Section 3.3.6, "About the Application Tier"
- Section 3.3.7, "About the Identity Stores"

3.3.1 About Exalogic Physical and Virtual Deployment Topologies

There are two types of Exalogic deployments. The first is a physical Exalogic deployment where each compute node in the Exalogic machine is used in its entirety. For more information see: *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

The second type is a virtual Exalogic deployment, where virtual servers are run on the Oracle Exalogic machine controlled by Oracle Enterprise Manager Ops Center. For more information, see: *Oracle Exalogic Elastic Cloud Machine Owner's Guide*, *Oracle Exalogic Elastic Cloud Administrator's Guide*.

This guide covers both deployment scenarios.

Physical Exalogic Deployment

A physical Exalogic Deployment uses the compute nodes directly. A dedicated compute node is a powerful entity and can fit the entire Oracle Traffic Director

(OTD)/Identity and Access Management (IAM) software stack onto a single compute node. This is why the Exalogic Physical topology is shown with all the products divided between a pair of compute nodes.

This design makes optimum use of the hardware. It does not, however, provide the most secure implementation.

If more security is required, the OTD servers can be placed onto a separate dedicated set of compute nodes which can be hidden behind a dedicated VLAN partition, creating a buffer between the outside world and the internal web applications.

Using two dedicated compute nodes for OTD is, however, expensive. Such a configuration makes more sense if the Exalogic machine is being used to host multiple applications, such as Identity and Access Management and WebCenter or SOA. In such a case, a single OTD configuration could be used as a front end for each of the different applications.

Virtual Exalogic Deployment

In a virtual Exalogic deployment, the Exalogic machine is configured to host virtual servers, whose load is distributed among the underlying compute nodes by means of the Exalogic Cloud Infrastructure, which is installed onto the Exalogic machine.

In a virtual Exalogic deployment, you do not need to use the full capabilities of the compute nodes, as it makes more sense to spread the topology over smaller, manageable virtual servers (vServers). The virtual server distribution has been chosen such that:

- OTD sits on dedicated servers, as they are responsible for routing requests to all components in the deployment
- There is a pair of vServers for each domain. This is consistent with the Split Domain ideal. That is, the access domain can be patched independently of the governance domain. When each domain is placed onto a dedicated server, it is possible to scale out just one domain, or to patch the OS on just one domain, without impacting another.

3.3.2 About EoIB and IPoIB Communication

When you initially set up your Exalogic machine, the default network is running IP over Infiniband (IPoIB). For the different purposes of the topology described in this guide, you must configure Ethernet over Infiniband (EoIB) network access in addition to the IPoIB network. For more information, see "Configuring Ethernet Over InfiniBand" in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

In an Exalogic deployment the two different types of network are used as follows:

- IPoIB is used for internal communications for components within the Exalogic machine rack. This network is not visible outside of the Exalogic machine rack itself.
- EoIB is used for components inside the Exalogic machine rack to communicate with components external to the Exalogic machine rack.

The following types of communication must be configured for the Oracle Identity and Access Management enterprise deployment on Exalogic:

- For the Oracle Traffic Director hosts, the IP addresses must be EoIB addresses accessible from the load balancer. The Oracle Traffic Director IP addresses are the only addresses accessible from the DMZ network.

- IAM Servers use IPoIB addresses as the main listen address for internal invocations and for RMI interactions inside the Exalogic rack.
- If the Database Server is accessible over EoiB, the application machines must be able to access external hosts on EoIB
- Communication and routing between Oracle Traffic Director hosts and the application tier must be only over IPoIB.
- For communication between the application tier components, for example, internal JMS destinations routing must be on IPoIB. Any front end address that is exposed ONLY for internal consumption, uses and IPoIB virtual IP on Oracle Traffic Director hosts.
- IAM Servers can also be accessed externally for RMI/JMS/T3 invocations and HTTP invocations. These take place for remote deployments, for external JMS producers and consumers and for other operations that use a listen address of the IAM servers that is available outside the Exalogic rack (EoIB).

For more information about IPoIB and EoIB network configuration, see Section 4, "Networking Overview."

3.3.3 About the Hardware Load Balancer

In an Exalogic deployment, a hardware load balancer sits outside the Exalogic machine rack. Its function is to receive external requests for the IAM deployment and pass them on to each of the Web hosts. These Web hosts can either be Oracle HTTP servers or Oracle Traffic Director servers.

The load balancers are configured to receive HTTP and HTTPS requests. If an HTTPS request is received at the load balancer, the SSL is decrypted at the load balancer and passed on to the Web Servers using the HTTP protocol. This is known as SSL Termination at the load balancer.

The communication from the hardware load balancer to the Web tier is entirely over EoIB.

The load balancer is used to route both application and administrative requests to the Web servers. Administrative requests originate inside the organization’s intranet. Application requests may be received through the intranet or the internet.

3.3.4 About the DMZ

A DMZ is a means of restricting access to components of your infrastructure to those that actually need it. In the examples in this guide, there is a public DMZ. This is where the outside world gains access to your systems. You place into this zone only those components that the outside world must access, such as the Load Balancers and Oracle HTTP Servers (if used in the topology). If users from the outside world attempts to access any servers or services below this zone, they are prevented from doing so by firewalls. The public zone is configured so that the servers in this zone can interact with the application servers in the private zone.

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

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

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

By using this approach, you restrict access to information to only those components that require it. This approach is useful where you have users coming in from outside of your organization. If, instead of an extranet, you are setting up an intranet, where all communication is from trusted sources, then you might reasonably decide to do away with the public DMZ.

3.3.5 About the Web Tier

Oracle Traffic Director can be used as the primary HTTP Server or in conjunction with Oracle HTTP Server. When used in conjunction with Oracle HTTP Server, Oracle Traffic Director only handles internal requests within the Exalogic machine.

The architecture of Oracle Traffic Director enables it to handle large volumes of application traffic with low latency. It is optimized for use in Oracle Exalogic Elastic Cloud. It communicates with WebLogic Servers in the back end over Exalogic's InfiniBand fabric (IPoIB).

3.3.5.1 Oracle Traffic Director Only

In this topology, the Oracle Traffic Director instances serve two purposes:

- The Oracle Traffic Director instances receive HTTP requests coming in from the hardware load balancer (over the EoIB network) and then route those requests (over the IPoIB network) to the compute nodes in the application tier.
- They route requests from the application tier components (over the IPoIB network) to other application tier components, such as requests from Oracle Access Manager to the Oracle Unified Directory directory service.

3.3.5.2 Oracle HTTP Server and Oracle Traffic Director

- The Oracle HTTP Servers receive requests coming in from the hardware load balancer and then route those requests (over the EoIB network) to the compute nodes in the application tier.
- The internal application to application requests, which are routed only over the internal IPoIB network, are routed through the Oracle Traffic Director via a virtual IP address that is depicted as VIP1 in the topology diagram (Figure 2–1).

3.3.5.3 More about Oracle Traffic Director

The Oracle Traffic Director instances are configured as part of a failover group. In this configuration, Oracle Traffic Director uses an implementation of the Virtual Routing Redundancy Protocol (VRRP) to provide failover capabilities. If an Oracle Traffic Director instance fails, IP addresses enabled on it are migrated to surviving instances, via VRRP. WebGate uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager to perform operations such as user authentication.

Oracle Traffic Director performs the following actions.

- Distributes the requests that it receives from clients to servers in the application tier based on the specific load-balancing method
- Routes the requests based on specified rules
- Caches frequently accessed data
- Prioritizes traffic and controls the quality of service

- Oracle Traffic Director can be used to route HTTP or LDAP requests

3.3.6 About the Application Tier

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

The application tier includes the following components, which are installed on Managed Servers in the Oracle WebLogic Server domains:

- Access Control services, which determine who has access to which resources. These services are provided by Oracle Access Manager.
- Fraud Detection services, which, when combined with Access Control ensure a higher level of security and fraud detection. This is provided by Oracle Adaptive Access Manager.
- Provisioning services, allowing users to request and manage accounts on the system. This is provided by Oracle Identity Manager and Oracle SOA.
- The Provisioning services are deployed into a separate domain to that of the Access Control services to facilitate independent management and patching.

IAMHOST1 hosts an Oracle WebLogic Administration Server. The Administration Server hosts the Oracle WebLogic Console, Oracle Enterprise Manager Fusion Middleware Control, Oracle Access Management Console, and Oracle Directory Services Manager (ODSM) for OUD.

Note that the Oracle WebLogic Server Administration Server is a singleton process. That is, only one Administration Server can be running at a time within a domain. In the event that the host running the Administration Server fails, the Administration Server can be manually started on a different host.

3.3.6.1 About Oracle Unified Directory Assured Replication

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

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

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

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

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

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

3.3.6.2 Architecture Notes

- An embedded version of Oracle Entitlement Server is used to control access to Oracle Fusion Middleware components.
- Oracle Entitlements Server uses a centralized policy store that is stored within a database.
- Access Manager uses the OPSS Policy Store to store policy information.
- The Oracle WebLogic Server console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Access Management console are always bound to the listen address of the Administration Server.
- Managed servers WLS_OAM1 and WLS_OAM2 are configured in a cluster.
- The managed servers WLS_OIM1 and WLS_OIM2 are configured in a cluster.
- The managed servers WLS_SOA1 and WLS_SOA2 are configured in a cluster.

3.3.6.3 High Availability Provisions

- Oracle Traffic Director can be configured for high availability in active-passive mode. Virtual Hosts/IP addresses are started on a single OTD instance. A heart beat exists between each OTD instance. Using this heart beat, a secondary OTD instance will enable the virtual host/IP address in the event of the failure of the primary OTD instance.
- OAM Server, Oracle Identity Manager, and SOA are active-active deployments; these servers communicate with the data tier at run time.
- Oracle Traffic Director directs HTTP and LDAP requests to all WebLogic managed servers or OUD Instances ensuring maximum availability.
- The WebLogic Administration Server and Oracle Enterprise Manager deployment is active-passive (where other components are active-active). There is one Administration Server per domain.
- The WebLogic Administration Server is a singleton component deployed in an active-passive configuration. If the primary fails or the Administration Server on IAMHOST1 does not start, the Administration Server on the secondary host can be started. If a WebLogic managed server fails, the node manager running on that host attempts to restart it.

For more information about Oracle Identity and Access Manager high availability, see "Configuring High Availability for Oracle Identity and Access Management Components" in the *Oracle Fusion Middleware High Availability Guide for Oracle Identity and Access Management*

3.3.6.4 Security Provisions

The administration tools for this deployment (for example, Oracle WebLogic Server Console, Oracle Enterprise Manager Fusion Middleware Control console, and Oracle Access Management Console) are accessible only through a virtual host, such as `iadadmin.mycompany.com`, which is a virtual host configured on the hardware load balancer. This is only available within the intranet.

3.3.7 About the Identity Stores

Identity information is stored in an LDAP compliant directory. In this topology, Oracle supports the Oracle Unified Directory natively.

3.4 About Oracle Directory Services Manager

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

3.5 Benefits of Using the Split Domain Topology

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

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

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

3.6 Hardware Requirements for the Identity Management on Exalogic

The following sections describe the hardware requirements for the Identity and Access Management enterprise topologies on Exalogic:

- Hardware Load Balancer Requirements
- Exalogic Machine Requirements

3.6.1 Hardware Load Balancer Requirements

The Oracle Fusion Middleware enterprise deployment requires a hardware load balancer to route requests to the Web tier. For information about the minimum set of features required for the load balancer in this topology, see Section 4.4.1, "Load Balancer Requirements."

3.6.2 Exalogic Machine Requirements

Exalogic machines consist of virtual or physical machines, a storage appliance, as well as required InfiniBand and Ethernet networking components. The number of these components in each machine varies based on the hardware configuration.

For complete information about the hardware options available for Exalogic machines, see "Exalogic Hardware Configurations" in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

For any of the topologies described in this guide, an Exalogic machine eighth rack can be used. For more information, see Section 3.2, "Understanding the Oracle Identity Management Deployment Topology on Exalogic".

Assign two machines to the Application Tier. These will be referred to as IAMHOST1 and IAMHOST2.

Note that you can also assign compute nodes for a standard Oracle RAC database, but this guide assumes your database will be hosted on a remote set of hosts.

3.7 Software Components for an Enterprise Deployment

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

This section contains the following topics:

- Section 3.7.1, "Software Required for the Oracle Identity Management Deployment Topology on Exalogic"
- Section 3.7.2, "About Obtaining Software"
- Section 3.7.3, "Mandatory Patches"
- Section 3.7.4, "Applying Patches and Work-arounds"

3.7.1 Software Required for the Oracle Identity Management Deployment Topology on Exalogic

Table 3–1 lists the Oracle software you need to obtain before starting the procedures in this guide.

Table 3–1 Software Versions Used

Short Name	Product	Version
OTD	Oracle Traffic Director	11.1.1.7.0
JRockit	Oracle JRockit	jrockit-jdk1.6.0_29-R28.2.0-4.0.1 or newer
WLS	Oracle WebLogic Server	10.3.6.0
IAM	Oracle Identity and Access Management	11.1.2.2.0
SOA	Oracle SOA Suite	11.1.1.7.0
WebGate	WebGate 11*g*	11.1.2.2.0
RCU	Repository Creation Assistant	11.1.2.2.0
OUD	Oracle Unified Directory	11.1.2.2.0
OHS	Oracle HTTP Server	11.1.1.7.0

3.7.2 About Obtaining Software

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

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

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

You must also download Oracle Traffic Director and Oracle WebGate for Oracle Traffic Director. Extract to `otd` and `webgate_otd` in: *`REPO_HOME`*`/installers`:

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

3.7.3 Mandatory Patches

Table 3–2 lists the patches required by Oracle Identity and Access Management on Exalogic.

Table 3–2 Mandatory Patch

Platform	Patch Number and Description on My Oracle Support
Generic Platform (2000)	18221571 ORACLE IDENTITY MANAGER BUNDLE PATCH 11.1.2.2.5

3.7.4 Applying Patches and Work-arounds

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

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

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

Download the patches from http://support.oracle.com and expand each patch to the directory appropriate for the product, as listed in Table 3–3. If the directory does not exist, create it.

After expanding the patch make sure that the Patch Directory (as listed in Table 3–3) contains a directory which is a number. That directory contains directories and files similar to:

- etc

- files
- README.txt

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

bundle_patch_no/*product*/*product_patch_no*

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

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

Table 3–3 Product Patch Directories

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

3.8 Road Map for the Reference Topology Installation and Configuration

Before beginning your Oracle Identity and Access Management enterprise deployment, review the flow chart in Figure 3–4, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process". This flow chart illustrates the high-level process for completing the enterprise deployment documented in this guide. Table 3–4 describes the steps in the flow chart and directs you to the appropriate section or chapter for each step.

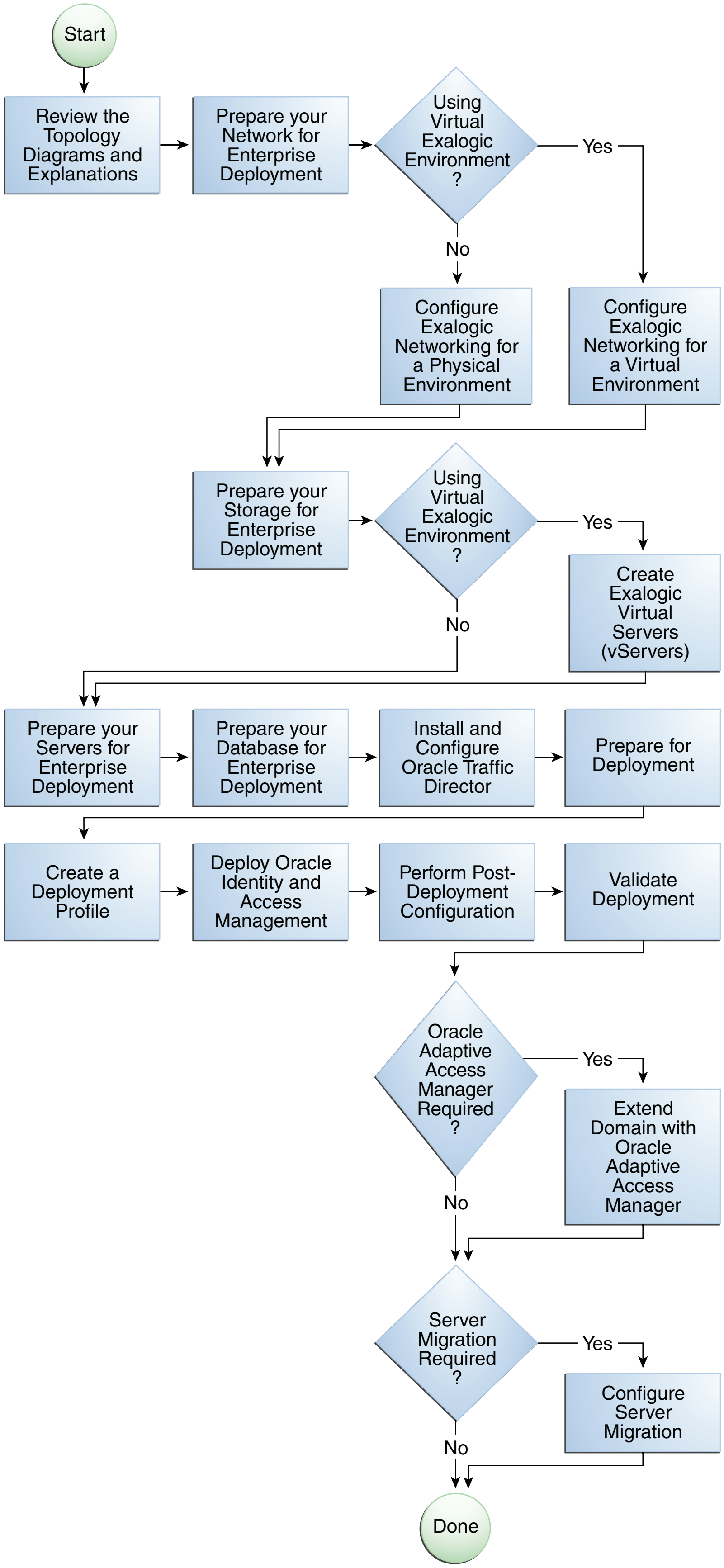
This section covers the following topics:

- Section 3.8.1, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process"
- Section 3.8.2, "Steps in the Oracle Identity and Access Management Enterprise Deployment Process"

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

Figure 3–4, "Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process" provides a flow chart of the Oracle Identity and Access Management enterprise deployment process. Review this chart to become familiar with the steps that you must follow, based on the existing environment.

Figure 3–4 Flow Chart of the Oracle Identity and Access Management Enterprise Deployment Process


Start
Review the Topology Diagrams and Explanations
Prepare your Network for Enterprise Deployment
Using Virtual Exalogic Environment ?
Yes
No
Configure Exalogic Networking for a Physical Environment
Configure Exalogic Networking for a Virtual Environment
Prepare your Storage for Enterprise Deployment
Using Virtual Exalogic Environment ?
Yes
No
Create Exalogic Virtual Servers (vServers)
Prepare your Servers for Enterprise Deployment
Prepare your Database for Enterprise Deployment
Install and Configure Oracle Traffic Director
Prepare for Deployment
Create a Deployment Profile
Deploy Oracle Identity and Access Management
Perform Post-Deployment Configuration
Validate Deployment
Oracle Adaptive Access Manager Required ?
Yes
No
Extend Domain with Oracle Adaptive Access Manager
Server Migration Required ?
Yes
No
Configure Server Migration
Done

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

Table 3–4 describes each of the steps in the enterprise deployment process flow chart for Oracle Identity and Access Management, shown in Figure 3–4. The table also provides information on where to obtain more information about each step in the process.

Table 3–4 Steps in the Oracle Identity and Access Management Enterprise Deployment Process

Step	Description	More Information
Review the Enterprise Deployment Topology	Review the recommended topology and plan the topology best suited for organization and applications.	Section 3.1, "Planning Your Deployment"
Prepare the Network for an Enterprise Deployment	To prepare your network for an enterprise deployment, understand concepts, such as virtual server names and IPs and virtual IPs, and configure your load balancer by defining virtual host names.	
Prepare your File Storage Appliance for an Enterprise Deployment	To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared storage.	
Prepare the Compute Nodes for an Enterprise Deployment	To prepare your servers for an enterprise deployment, ensure that your servers meet hardware and software requirements, enable Unicode support and Virtual IP Addresses, mount shared storage, configure users and groups, and, if necessary, install software onto multi-homed systems.	
Prepare the Oracle RAC Database for an Enterprise Deployment	To prepare an Oracle RAC database for an enterprise deployment, review database requirements, create database services, load the metadata repository, in the Oracle RAC database, configure Identity and Access Management schemas for transactional recovery privileges, and back up the database.	
Install and Configure Oracle Unified Directory	Install and configure Oracle Unified Directory, which is used as the Identity Store in the recommended topologies. Configure two instances of Oracle Unified Directory by using Oracle Unified Directory configuration assistant.	
Create the Initial WebLogic Server Domain	Run the Configuration Wizard to create the initial WebLogic Server domain.	
Install and Configure Oracle Traffic Director on Exalogic Compute Nodes	Install and configure Oracle Traffic Director.	

Table 3–4 (Cont.) Steps in the Oracle Identity and Access Management Enterprise Deployment Process

Step	Description	More Information
Extend the Domain for Oracle Access Management?	Run the Configuration Wizard again and extend the domain to include Oracle Access Management.	
Extend the Domain for Oracle Identity Manager?	Run the Configuration Wizard again and extend the domain to include Oracle Identity Manager.	
Configure SSO for the Administration Console	Configure single sign-on (SSO) for administration consoles in an Identity and Access Management Enterprise deployment.	
Configure Node Manager	Set up Node manager by enabling host name verification, starting Node Manager, and configuring WebLogic Servers to use custom keystores.	
Configure Server Migration	Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers. The WLS_OIM1 and WLS_SOA1 Managed Server are configured to restart on IAMHOST2 should a failure occur. The WLS_OIM2 and WLS_SOA2 Managed Servers are configured to restart on IAMHOST1 should a failure occur.	

4 Networking Overview

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

This chapter includes the following topics:

- Section 4.1, "Overview of Preparing the Network for an Enterprise Deployment"
- Section 4.2, "Planning Your Network"
- Section 4.3, "Virtual Server Names Used by the Topology"
- Section 4.4, "Configuring the Hardware Load Balancers"
- Section 4.5, "About IP Addresses and Virtual IP Addresses"
- Section 4.6, "Configuring Firewall Ports"
- Section 4.7, "Managing Access Manager Communication Protocol"
- Section 4.8, "Exalogic Networking"

4.1 Overview of Preparing the Network for an Enterprise Deployment

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

4.2 Planning Your Network

As shown in the deployment topology figures in Section 3.2, "Understanding the Oracle Identity Management Deployment Topology on Exalogic," each deployment can be spread across multiple zones. A zone is a means of restricting access to components of your infrastructure to those that actually need it. In the examples in this guide, two zones are shown.

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

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

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

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

In an Exalogic Deployment the use of Zones can be achieved by using different VLANs.

4.3 Virtual Server Names Used by the Topology

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

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

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

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

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

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

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

Both:

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

Exalogic:

With Exalogic, these IP Addresses may be associated with Oracle Traffic director.

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

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

You define the virtual server names on the load balancer using the procedure in Section 4.4, "Configuring the Hardware Load Balancers"

The rest of this guide assumes that the deployment is one of those shown in Chapter 3, "Introduction and Planning."

4.3.1 IDSTORE.mycompany.com

- Because your Identity Store in Oracle Unified Directory is accessed directly, you must monitor the heartbeat of the Oracle Unified Directory processes. If an Oracle Unified Directory process stops, the load balancer must continue to route the LDAP traffic to a surviving Oracle Unified Directory instance.
- This virtual server directs traffic received on port 1489 *(LDAP_LBR_PORT)* to each of the Oracle Unified Directory instances on port 1389 (*LDAP_DIR_PORT*).
- This virtual server directs traffic received on port 1636 (*LDAP_LBR_SSL_PORT*) to each of the Oracle Unified Directory instances on port 1636 *(LDAP_DIR_SSL_PORT*).
- This virtual server is resolvable only locally (in Exalogic).
- In an Exalogic Deployment, IDSTORE load-balancing is undertaken by Oracle Traffic Director.

4.3.2 IADADMIN.mycompany.com

- This virtual server acts as the access point for all internal HTTP traffic that gets directed to the administration services in the Access Domain. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `IADADMIN.mycompany.com:80` and in turn forward these to port 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2, or OHSHOST1 and OHSHOST2 on the Exalogic OHS Topology. The services accessed on this virtual host include the WebLogic Administration Server Console and Oracle Enterprise Manager Fusion Middleware Control.
- This virtual server is resolvable in the corporate DNS only.
- Create rules in the firewall to block outside traffic from accessing the `/console`, `/oamconsole`, `/oaam_admin`, and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IADADMINVHN.mycompany.com` virtual host.

4.3.3 IGDADMIN.mycompany.com

- This virtual server acts as the access point for all internal HTTP traffic that gets directed to the administration services in the Governance Domain. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `IGDADMIN.mycompany.com:80` (*`HTTP_PORT`*) and in turn forward these to ports 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2 or OHSHOST1 and OHSHOST2 in the Exalogic OHS Topology. The services accessed on this virtual host include the WebLogic Administration Server Console, and Oracle Enterprise Manager Fusion Middleware Control,and Oracle Authorization Policy Manager.
- Create rules in the firewall to block outside traffic from accessing the `/sysadmin`, `/apm`, `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IGDADMINVHN.mycompany.com` virtual host.

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

4.3.4 IDMINTERNAL.mycompany.com

- This virtual server acts as the access point for all internal HTTP traffic that gets directed to OIM and SOA. The incoming traffic from clients is not SSL enabled. The the clients access this service using the address `idminternal.mycompany.com:80` and Oracle Traffic Director in turn forwards these to the appropriate WebLogic managed servers.
- Create rules in the firewall to block outside traffic from accessing this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `IDMINTERNAL.mycompany.com` virtual host.
- This virtual server should be resolvable either locally or in the corporate DNS
- Because `IDMINTERNAL` is designed for interprocess communication, you might want to NOT include this in DNS, but have it resolvable only in internal host files.
- In an Exalogic Deployment, `IDMINTERNAL` load-balancing is undertaken by Oracle Traffic Director.

4.3.5 SSO.mycompany.com

- This is the virtual name which fronts all Identity and Access Management components, including Access Manager and Oracle Identity Manager.
- This virtual server acts as the access point for all HTTP traffic that gets directed to the single sign on services. The incoming traffic from clients is SSL enabled. Thus, the clients access this service using the address `SSO.mycompany.com:443` and in turn forward these to port 7777 (*WEB_HTTP_PORT*) on WEBHOST1 and WEBHOST2 or OHSHOST1 and OHSHOST2 in the Exalogic OHS Topology. All the single sign on enabled protected resources are accessed on this virtual host.
- Configure this virtual server in the load balancer with both port 80 (*HTTP_PORT*) and port 443 (*HTTP_SSL_PORT*).
- This virtual server should be resolvable either locally or in the corporate DNS
- This virtual host must be configured to preserve the client IP address for a request. In some load balancers, you configure this by enabling the load balancer to insert the original client IP address of a request in an X-Forwarded-For HTTP header.

4.4 Configuring the Hardware Load Balancers

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

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

When configuring a load balancer, you must set up a virtual host for each of the virtual servers, as described in Section 4.4.3, "Load Balancer Configuration for Exalogic."

In an Exalogic implementation some of these virtual servers will be enabled on Oracle Traffic Director rather than on the Load balancer.

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

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

This section contains the following topics:

- Section 4.4.1, "Load Balancer Requirements"
- Section 4.4.2, "Load Balancer Configuration Procedures"
- Section 4.4.3, "Load Balancer Configuration for Exalogic"

4.4.1 Load Balancer Requirements

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

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

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

4.4.2 Load Balancer Configuration Procedures

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

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

4.4.3 Load Balancer Configuration for Exalogic

For an Identity Management deployment, configure your load balancer as shown in Table 4–1.

Table 4–1 Load Balancer Configuration Details

Virtual Servers	Server Pool[1]	Server Pool (External OHS)	Protocol	SSL Termination	External	Other Required Configuration/Comments
SSO.mycompany.com:80 (*HTTP_SSL_PORT*)	WEBHOST1VHN1.mycompany.com:7777 WEBHOST2VHN1.mycompany.com:7777	OHSHOST1.mycompany.com:7777 OHSHOST2.mycompany.com:7777	HTTP	No	Yes	
SSO.mycompany.com:443 (*HTTP_SSL_PORT*)	WEBHOST1VHN1.mycompany.com:7777 WEBHOST2VHN1.mycompany.com:7777	OHSHOST1.mycompany.com:7777 OHSHOST2.mycompany.com:7777	HTTP	Yes	Yes	Identity Management requires that the following be added to the HTTP header: Header Name: IS_SSL[2] Header Value: ssl Header Name: WL-Proxy-SSL Header Value: true
IADADMIN.mycompany.com:80 *HTTP_PORT*	WEBHOST1VHN1.mycompany.com:7777 WEBHOST2VHN1.mycompany.com:7777	OHSHOST1.mycompany.com:7777 OHSHOST2.mycompany.com:7777	HTTP	No	No	
IGDADMIN.mycompany.com:80 *HTTP_PORT*	WEBHOST1VHN1.mycompany.com:7777 WEBHOST2VHN1.mycompany.com:7777	OHSHOST1.mycompany.com:7777 OHSHOST2.mycompany.com:7777	HTTP	No	No	

[1] If you do not want to use an OTD failover group for faster failover detection, substitute WEBHOST1-VHN and WEBHOST2-VHN with the host names corresponding to the client access network. For example: IAMHOST1EXT and IAMHOST2EXT.

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

4.5 About IP Addresses and Virtual IP Addresses

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

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

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

- IADADMINVHN.mycompany.com

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

- IGDADMINVHN.mycompany.com

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

- SOAHOSTxVHN.mycompany.com

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

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

- OIMHOSTxVHN.mycompany.com

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

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

Configure the Administration Server and the managed servers to listen on different virtual IPs and physical IPs as illustrated in Figure 4–1.

Figure 4–1 Exalogic Physical IP Addresses and VIP Addresses

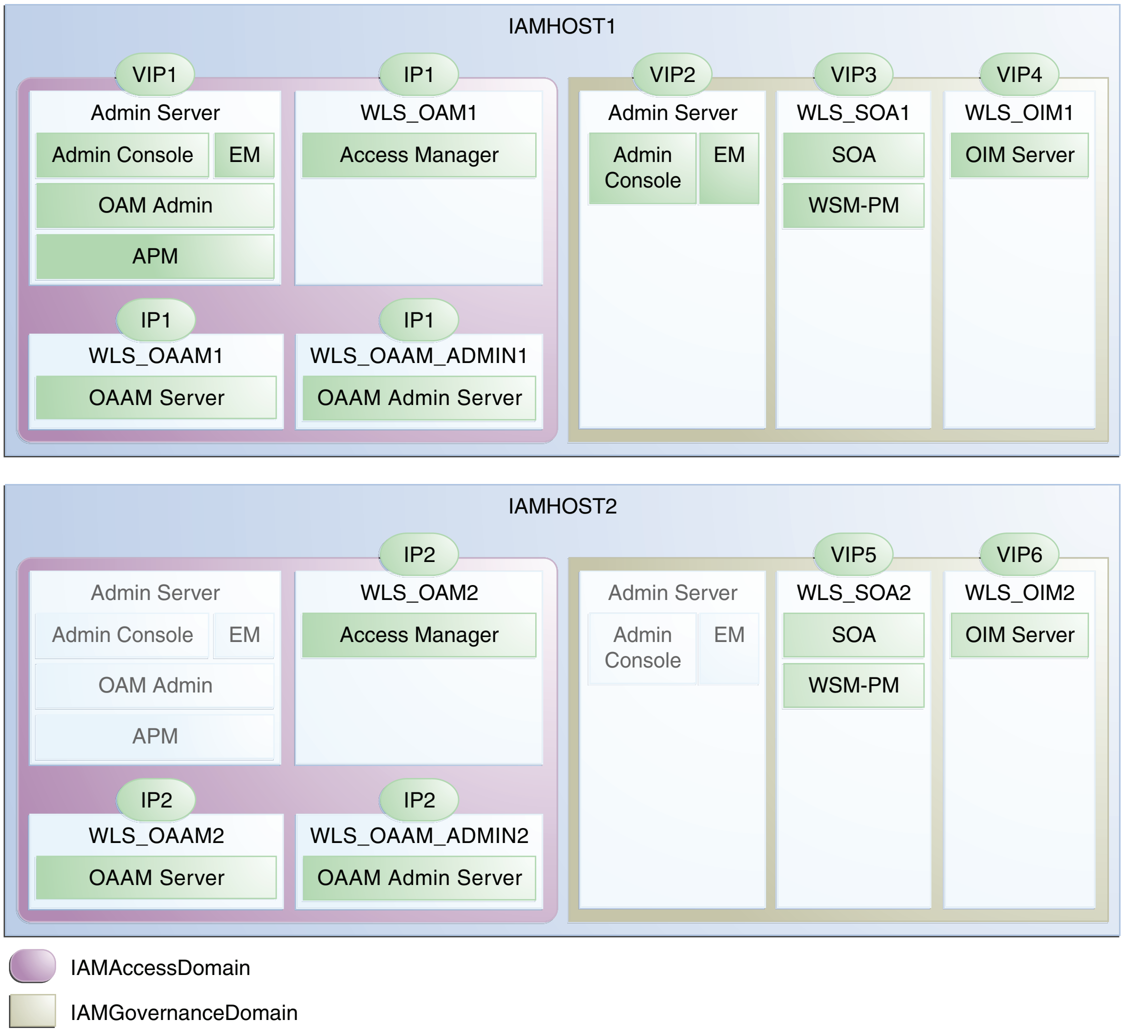
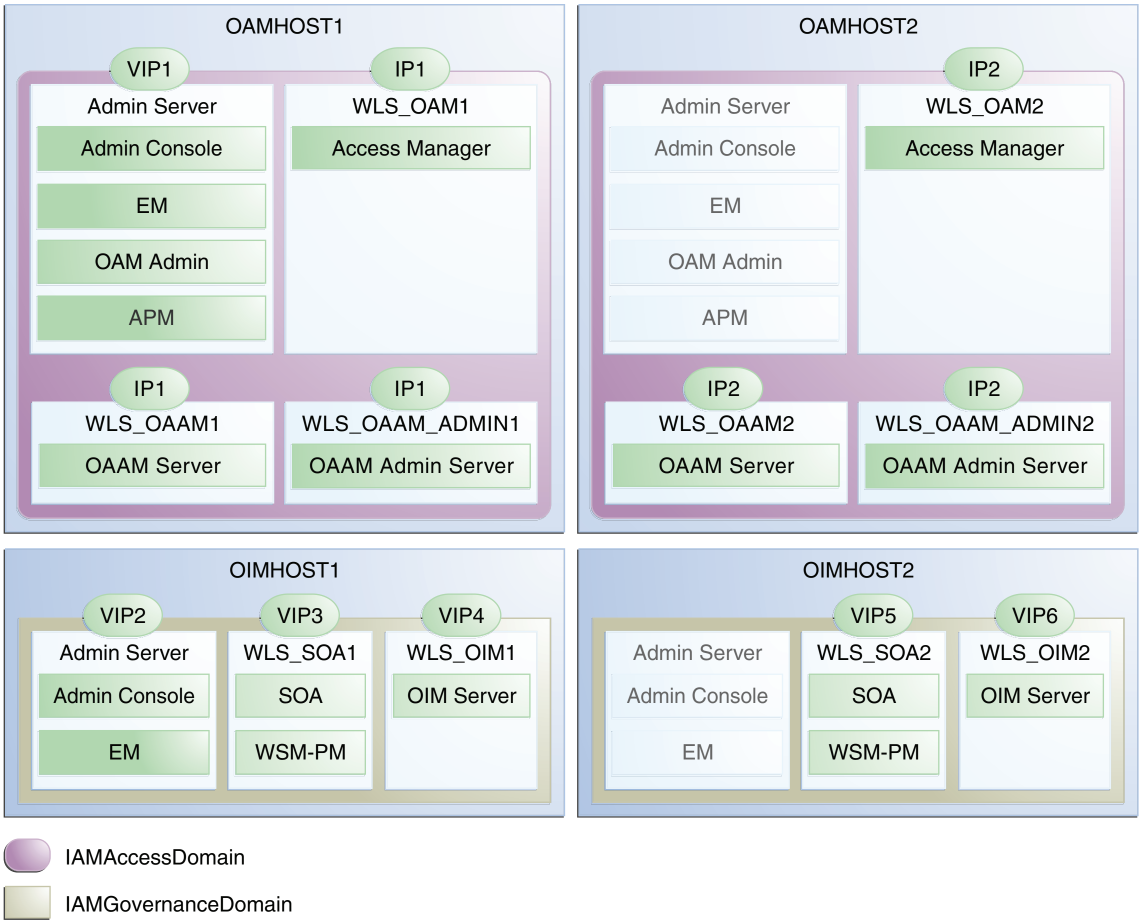


Figure 4–2 IP Addresses and VIP Addresses–Exalogic Virtual



The following table provides descriptions of the various virtual hosts.

Table 4–2 Exalogic VIP Addresses and Virtual Hosts

Virtual IP	VIP Maps to...	Description (Consolidated)	Default Host (Physical)	Default Host (Virtual)
VIP1	IADADMINVHN	IADADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running.	IAMHOST1	OAMHOST1
VIP2	IGDADMINVHN	IGDADMINVHN is the virtual host name that is the listen address for the Oracle Identity Manager Administration Server. It fails over with manual failover of the Administration Server. It is enabled on the node where the Oracle Identity Manager Administration Server process is running.	IAMHOST1	OIMHOST1
VIP3	SOAHOST1VHN	SOAHOST1VHN is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA1 process is running.	IAMHOST1	OIMHOST1

Table 4–2 (Cont.) Exalogic VIP Addresses and Virtual Hosts

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

4.6 Configuring Firewall Ports

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

Most port numbers are assigned during installation.

Table 4–3, " Ports Used in the Exalogic Reference Topology" lists the ports used in the Oracle Exalogic deployment reference topology, including the ports that you must open on the firewalls in the topology.

Firewall notation:

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

Table 4–3 Ports Used in the Exalogic Reference Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
Load balancer to Oracle Traffic Director	n/a	7777	HTTP	n/a	Timeout depends on all HTML content and the process models used for the Oracle Fusion Middleware products you are using in the Exalogic environment.
IAMAccess Domain Administration Console access	FW1	7001	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
IAMAccess Domain Administration Console SSL access	FW1	7002	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
IAMGovernance Domain Administration Console access	FW1	7101	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).

Table 4–3 (Cont.) Ports Used in the Exalogic Reference Topology

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
IAMGovernance Domain Administration Console SSL access	FW1	7102	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Coherence	n/a	8088 Range: 8080 - 8090		n/a	n/a
Application tier to data tier (Oracle database or RAC outside of Oracle Exalogic machine via Ethernet)	FW2	1521		n/a	n/a
Managed Server Access (WLS_OAM1, WLS_OAM2, WLS_OIM1. WLS_OIM2, WLS_SOA1, WLS_SOA2)	FW1	WLS_OAM*n*: 14100 WLS_OIM*n*: 14000 WLS_SOA*n*: 8001	HTTP	Inbound	Managed Servers, which use `bond1` floating IP addresses, are accessed via Oracle HTTP Server. Only required if the topology has external Oracle HTTP Servers.

4.7 Managing Access Manager Communication Protocol

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

This section contains the following topics:

- Section 4.7.1, "Access Manager Protocols"
- Section 4.7.2, "Overview of Integration Requests"
- Section 4.7.3, "Overview of User Request"
- Section 4.7.4, "About the Multicast Requirement for Communication"

4.7.1 Access Manager Protocols

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

4.7.2 Overview of Integration Requests

Oracle Access Management Access Manager is responsible for creating sessions for users. When Access Manager is integrated with another Identity and Access

Management component, such as Oracle Identity Manager, authentication is delegated to that component.

A typical request flow is as follows:

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

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

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

4.7.3 Overview of User Request

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

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

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

4.7.4 About the Multicast Requirement for Communication

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

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

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

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

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

4.8 Exalogic Networking

This section describes details of Exalogic Networking.

This section includes the following topics:

- Section 4.8.1, "Map of the Network Interfaces Used by the Components of the IAM Topology on Exalogic"
- Section 4.8.2, "Preparing the Network for an Exalogic Enterprise Deployment"

4.8.1 Map of the Network Interfaces Used by the Components of the IAM Topology on Exalogic

As described in Chapter 2, "Introduction to Oracle Identity and Access Management on Exalogic," the Exalogic Machine has a number of networks. In an Exalogic deployment, network traffic is confined to the internal network as much as is possible. This ensures that network traffic is not flooding the corporate network and adds an extra layer of security by ensuing host name resolution is only available where it is needed. For example `idminternal` is only resolvable inside the exalogic machine, this prevents direct corporate access using this communication channel.

Table 4–4 shows how the communication of Oracle Identity and Access components use these networks. Sample IP address ranges have been used to differentiate the different IP Address usages.

Where possible, different vnets are used to further compartmentalise network traffic.

Table 4–4 Internal and External IP Addresses

Purpose	Network	IP Addresses	Netmask
External Compute Node Addresses	EoIB	10.10.10.x	255.255.224.0
External Floating Physical IP Addresses	EoIB	10.10.30.x	255.255.224.0
External Floating Oracle Traffic Director IP Addresses	EoIB	10.10.50.x	255.255.224.0
Internal Compute/vServer Node Addresses	IPoIB	192.168.10.x	255.255.224.0
Internal Storage Addresses	IPoIB	192.168.32.x	255.255.224.0
Exadata Network	IPoIB	192.168.10.x	255.255.224.0
Internal Floating Physical IP Addresses	IPoIB	192.168.30.x	255.255.240.0
Internal Oracle Traffic Director Addresses	IPoIB	192.168.50.x	255.255.224.0

Notes:

- The external IP addresses in Table 4–4 are assumed to be on the client access network.
- The subnets used here are examples only. It may be possible to use these subnets, the externally facing subnets. Follow the standards used in your organization. In virtual Exalogic, internal network IP addresses are determined by the Exalogic Elastic Cloud software when a private network is created. These are referred to as bond*x* (where *x* is a sequential number).

For more information about the network map diagram, see the following:

- Table 9–3, " Logical Virtual IP Addresses Associated with IPoIB Network interfaces" lists the IPoIB (bond0) interfaces required for each compute node, as well as suggested IP addresses to assign to each interface.
- Table 5–3, " IP Addresses for the EoIB Network and Associated Interfaces" lists the EoIB (bond1) interfaces required for each compute node, as well as the suggested IP addresses to assign to each interface.

4.8.2 Preparing the Network for an Exalogic Enterprise Deployment

To continue preparing your network, refer to either Chapter 5, "Configuring Exalogic Networking for a Physical Environment" or Chapter 6, "Configuring Exalogic Networking for a Virtual Environment," depending on which type of environment you are configuring.

5

Configuring Exalogic Networking for a Physical Environment

This chapter describes Physical Exalogic Networking.

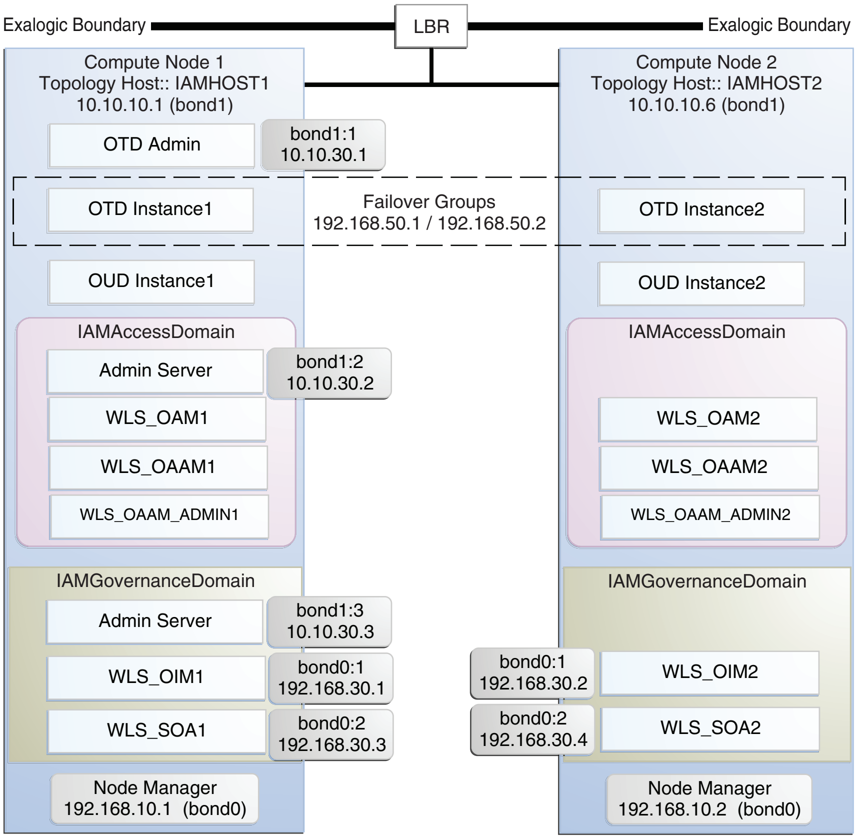
The contents in this chapter are specific to the Exalogic physical environment and should be read in conjunction with the Chapter 4, "Networking Overview."

This chapter contains the following sections:

5.1 Network Map

The following image illustrates the IPoIB and EoIB network interfaces needed for an Oracle Identity Management enterprise deployment. The sections that follow provide a detailed description of the image.

Figure 5–1 Physical Exalogic Network Map



5.2 Explanation of the Network Interfaces Map

In a physical Exalogic deployment, A hardware load balancer distributes requests to two compute nodes in the Exalogic Rack. All of the Identity Management and Oracle Traffic Director software is deployed across these two compute nodes in a highly available fashion. Figure 5–1 shows how these compute nodes are networked together and to the external corporate network where the load balancer sits

This section contains the following topics:

- Section 5.2.1, "Load Balancer"
- Section 5.2.2, "Network Interface Bonding"
- Section 5.2.3, "Oracle Traffic Director"
- Section 5.2.4, "External Oracle HTTP Servers"
- Section 5.2.5, "Compute Nodes"

5.2.1 Load Balancer

An external load balancer sits outside of the exalogic machine rack. Its purpose is to receive requests on the public ethernet network and distribute those requests to the Oracle Traffic Director nodes inside the machine rack using the front end EoIB network or to the external Oracle HTTP Servers.

5.2.2 Network Interface Bonding

In order to maintain maximum availability, individual network interfaces are bonded together so that the failure of one interface will not affect the availability of the system.

In Physical Exalogic Deployments the following network bonding is assumed:

Network Interface	Purpose
bond0	This is the internal network used for communication between applications and with Exadata (if used).
bond1	This is the external client access network

These are the default network interfaces all of which have an associated IP address. Virtual IP addresses can temporarily be added to these network interfaces as required by the IAM deployment. Virtual IP addresses are shown as `:x` where `x` is a sequential number. For example `bond1:1`.

5.2.3 Oracle Traffic Director

Oracle Traffic Director (OTD) serves two functions: load balancing, and HTTP server.

As a load balancer, Oracle Traffic Director is configured in a way that it can direct requests to the Oracle Unified Directory servers using the internal IPoIB network using TCP and to direct internal call back requests from Oracle Traffic Director to SOA servers using the internal IPoIB network using HTTP.

Unless External Oracle HTTP Servers are used, then Oracle Traffic Director also functions as an HTTP Server. Oracle Traffic Director listens on the front end EoIB network for HTTP requests originating from the external load balancers. If these requests require access to the WebLogic managed servers on the compute nodes, then it directs these requests accordingly using the internal IPoIB network.

5.2.4 External Oracle HTTP Servers

Optionally, you can use Oracle HTTP Servers, which sit on servers outside of the Exalogic machine rack. These servers receive requests from the load balancer and distribute those requests to application compute nodes inside the machine rack using EoIB. All internal traffic still takes place using IPoIB and Oracle Traffic Director.

External HTTP Servers may be required in organizations that need to place the Web Tier in a separate DMZ than the Exalogic machine. Or have other applications or policies that require an HTTP Server.

5.2.5 Compute Nodes

In an Exalogic Physical deployment, the physical compute nodes are used to host services.

The following sections describe the networking configuration of each of the Compute Nodes in the deployment.

5.2.5.1 ComputeNode1

ComputeNode1 serves two purposes. It hosts Oracle Traffic director, which acts as both an internal load balancer and a web server. It also hosts the Oracle Identity and Access Management Applications which comprise Access Manager, Oracle Identity Manager and Oracle Unified Directory.

- It is configured to use the EoIB client access network. It uses this network to communicate with the external load balancer.
- It is configured to use the IPoIB network for internal communications.
- Oracle Traffic Director enables an IP address using a failover group to route requests to the Oracle Unified Directory servers using the IPoIB network.
- Oracle Traffic Director acts as a failover node in the event that the IP address used for internal callbacks fails.
- Oracle Traffic Directory is used to route application requests to the Weblogic managed servers making up the Application Tier.
- Node Manager, which is used to start and stop the WebLogic managed servers is configured to accept requests on the internal IPoIB interface.
- This node hosts virtual (floating) IP addresses which are configured on the client access network. These virtual IP addresses are used by the administration servers. Although not necessary to use the client access network. The benefit of doing so is that it is possible to monitor the administration servers outside of the Exalogic machine.
- Two virtual (floating) IP addresses are attached to the IPoIB interface, which are used by the Oracle Identity Manager and SOA managed servers to facilitate server migration.
- Oracle Unified Directory listens for requests on the internal IPoIB network.

5.2.5.2 ComputeNode2

ComputeNode2 serves 2 purposes. It hosts Oracle Traffic director, which acts as both an internal load balancer and a web server. It also hosts the Oracle Identity and Access Management Applications, which comprise Access Manager, Oracle Identity Manager and Oracle Unified Directory.

- It is configured to use the EoIB client access network. It uses this network to communicate with the external load balancer.
- It is configured to use the IPoIB network for internal communications.
- Oracle Traffic Director enables an IP address using a failover group to route internal callback requests to SOA servers using the IPoIB network.
- Oracle Traffic Director acts as a failover node in the event that the IP address used for Oracle Unified Directory fails.
- Oracle Traffic Directory is used to route application requests to the WebLogic managed servers making up the Application Tier.
- Node Manager, which is used to start and stop the local WebLogic managed servers is configured to accept requests on the internal IPoIB interface.
- This node hosts virtual (floating) IP addresses which are configured on the client access network. These virtual IP addresses are used by the administration servers. Although not necessary to use the client access network. The benefit of doing so is that it is possible to monitor the administration servers outside of the Exalogic machine.
- Two virtual (floating) IP addresses are attached to the IPoIB interface, which are used by the Oracle Identity Manager and SOA managed servers to facilitate server migration.
- Oracle Unified Directory listens for requests on the internal IPoIB network.

5.3 Host Name and Networking Overview

Networking is a complicated but critical part of any Exalogic deployment. This guide utilizes the IPoIB network for internal communications and the EoIB network for external communications.

Table 5–1, " Exalogic Physical IP Addresses Worksheet" is a summary of the required networking setup in the Exalogic physical machine rack. The following sections describe in detail how to set up this networking.

A column has been added to the table to allow you to add your own values for easier cross referencing.

Appropriate host name resolution is critical to topology designs that can sustain network changes, system relocation and disaster recovery scenarios. It is important that the required DNS (either `/etc/hosts` or central DNS server) definitions are in place and that WebLogic Servers use host names and virtual host names instead of using IP addresses and virtual IP addresses directly. Additionally, the Exalogic enterprise deployment requires a set of virtual server names for routing requests to the proper server or service within the topology through the external load balancer and the Oracle Traffic Director servers. See Section 4.3, "Virtual Server Names Used by the Topology."

These virtual server names must be resolvable in the corporate network. IPoIB addresses must be resolved only inside the rack's name resolution system. If multiple racks are going to be connected, to elude possible IP conflict, it is good practice to place these also in a central DNS server. Network administrators at the corporate level should enable this. Alternatively host names may be resolved through appropriate `/etc/hosts` file propagated through the different nodes. Table 5–1, " Exalogic Physical IP Addresses Worksheet" provides an example of names for the different floating IP addresses used by servers in the SOA system.

Table 5–1 Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IAMHOST1	bond0	192.168.10.1/255.255.224.0		IPoIB/ Fixed	ComputNode1 /IAMHOST1	NA	Access t IAMHO the inter network
IAMHOST2	bond0	192.168.10.2/255.255.224.0		IPoIB/ Fixed	ComputNode2 /IAMHOST2	NA	Access t IAMHO the inter network
OTDADMIN VHN	bond1:1	10.10.30.1/255.255.224.0		EoIB /Floating	ComputNode1 /IAMHOST1	OTD Administration Server	A floatin address Adminis Server is recomm you wan manuall the OTD Adminis Server fr IAMHO IAMHO

Table 5–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IADADMIN VHN	bond1:2	10.10.30.2/255.255.224.0		EoIB /Floating	ComputNode2 /IAMHOST1	IAMAccessDomain Administration Server	A floating IP address for the IAMAccessDom n Administratio Server is recommended, you want to manually migra the Administrat Server from IAMHOST1 to IAMHOST2.
IGDADMIN VHN	bond1:3	10.10.30.3/255.255.224.0		EoIB /Floating	ComputNode1 /IAMHOST1	IAMGovernanceDomain Administration Server	A floating IP address for the IAMGovernanc omain Administration Server is recommended, you want to manually migra the Administrat Server from IAMHOST1 to IAMHOST2.
WEBHOST1 VHN	OTD	10.10.50.1/255.255.224.0		EoIB /Floating	ComputNode1 /IAMHOST1	OTD - IAMHOST1	A floating IP Address manag by OTD. This is the IP Address which load balancers will connect.
WEBHOST2 VHN	OTD	10.10.50.2/255.255.224.0		EoIB /Floating	ComputNode2 /IAMHOST2	OTD - IAMHOST2	A floating IP Address manag by OTD. This is the IP Address which load balancers will connect. This is optional
OIMHOST1 VHN	bond0:1	192.168.30.1/255.255.240.0		IPoIB/ Floating	ComputNode1 /IAMHOST1	WLS_OIM1 Default Channel	Initially enablec IAMHOST1 car failed over by server migratior to IAMHOST2.
OIMHOST2 VHN	bond0:1	192.168.30.2/255.255.240.0		IPoIB/ Floating	ComputNode2 /IAMHOST2	WLS_OIM2 Default Channel	Initially enablec IAMHOST2 car failed over by server migratior to IAMHOST1.
SOAHOST1 VHN	bond0:2	192.168.30.3/255.255.240.0		IPoIB/ Floating	ComputNode1 /IAMHOST1	WLS_SOA1 default channel	Initially enablec IAMHOST1 car failed over by server migratior to IAMHOST2.

Table 5–1 (Cont.) Exalogic Physical IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
SOAHOST2 VHN	bond0:2	192.168.30.4/255.255.240.0		IPoIB/ Floating	ComputNode2 /IAMHOST2	WLS_SOA2 default channel	Initially Comput can be fa by serve migratio IAMHO
IAMHOST1 EXT	bond1	10.10.10.1/255.255.240.0		EoIB/Fixed	ComputNode1 /IAMHOST1	NA	A fixed allowing compute be acces External balancer
IAMHOST2 EXT	bond1	10.10.10.2/255.255.240.0		EoIB/Fixed	ComputNode2 /IAMHOST2	NA	A fixed allowing compute be acces External balancer
IDMINTERNAL	OTD	192.168.50.1/255.255.224.0		IPoIB/ Floating	ComputNode1 /IAMHOST1	NA	Oracle T Director group fo
IDSTORE	OTD	192.168.50.2/255.255.224.0		IPoIB/ Floating	ComputNode2 /IAMHOST2	NA	Oracle T Director group fo Unified

---

Note: In Table 5–1, where the interface is shown as **OTD**, means that the IP address is managed by Oracle Traffic Director rather than assigned to a network interface manually. The entries are included in this table for completeness.

5.4 Additional Requirements for External OHS

If External OHS Servers are being used then the additional host names in the following table apply to an Exalogic Physical configuration.

Table 5–2 Exalogic Physical OHS Configuration Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OHSHOST1	eth0	201.19.23.10/255.255.255.0		ETH0/Fixed	External OHSHOST1	Oracle HTTP Server	Fixed IP that Oracle HTTP Server Listens or
OHSHOST2	eth0	201.19.23.11/255.255.255.0		ETH0/Fixed	External OHSHOST2	Oracle HTTP Server	Fixed IP that Oracle HTTP Server Listens or

Table 5–2 (Cont.) Exalogic Physical OHS Configuration Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST1 VHN-EXT	bond1:2	10.10.10.7/255.255.255.224.0		EoIB/Floating	ComputeNode 1/IAMHOST1	WLS_OIM1 Default External Channel	Initially enabled on Compute Node 1, can be failed over to Compute Node 2
OIMHOST2 VHN-EXT	bond1:2	10.10.10.8/255.255.255.224.0		EoIB/Floating	ComputeNode 2/IAMHOST2	WLS_OIM2 Default External Channel	Initially enabled on Compute Node 2, can be failed over to Compute Node 1

Note: OIMHOSTxVHN-EXT is used in the external Oracle HTTP Server topology instead of the standard OIMHOSTxVHN entries used in the standard topologies. The -EXT is used to show that in an Oracle HTTP Server topology the OIMHOSTxVHN is bound to the client access network, rather than the internal network as used in the other topologies.

5.5 Preparing the Network on Physical Exalogic

By default, compute nodes are not able to communicate outside of the Exalogic machine rack. In order to do this you must configure the EoIB network for those hosts that are accessed via external hosts or load balancers.

The Oracle IAM hosts that require this access are *IAMHOST1* and *IAMHOST2*, which interact with an external load balancer, external database, or Oracle HTTP Server access.

This section contains the following topics:

- Section 5.5.1, "Summary of the IP Addresses for the EoIB Network Interfaces"
- Section 5.5.2, "Step 1 - Gather Information"
- Section 5.5.3, "Step 2 - Create a Virtual LAN"
- Section 5.5.4, "Step 3 - Create Virtual Network Cards"
- Section 5.5.5, "Step 4 - Configure Compute Node Networking and Assign Physical IP Address"

5.5.1 Summary of the IP Addresses for the EoIB Network Interfaces

Table 5–3, " IP Addresses for the EoIB Network and Associated Interfaces" lists the IP addresses you must associate with each EoIB interface on each compute node. Each of these interfaces is shown in Figure 5–1, "Physical Exalogic Network Map".

Table 5–3 IP Addresses for the EoIB Network and Associated Interfaces

Compute Node	Host Name	Interface Name	External IP Address	Netmask	Used by
ComputeNode1	IAMHOST1 EXT	bond1	10.10.10.1	255.255.224.0	Compute node for external load balancer access
ComputeNode2	IAMHOST2 EXT	bond1	10.10.10.2	255.255.224.0	Compute Node for external load balancer access

Configuring the EoIB network is a multi-stage process:

- Stage 1 - Determine the information required to create the network devices.
- Stage 2 - Create a Virtual LAN (VLAN) on the InfiniBand gateway switches for the compute nodes to communicate.
- Stage 3 - Create Virtual Network Cards on the InfiniBand gateway switches which can be seen by the compute nodes, allowing the compute nodes to utilize the EoIB network.
- Stage 4 - Configure the compute nodes to communicate using the VNICS by assigning IP addresses to them.

5.5.2 Step 1 - Gather Information

The following section describes how to gather the information required to create the VLAN and VNICs. To make things easier, complete the following worksheet as you are progressing:

Table 5–4 VNIC Worksheet

Compute Node	Administrative /External IP Address	Base Lid	GUID	Switch Lid	Switch Name	Connector	Switch GUID	MAC Address
IAMHOST1								
IAMHOST2								

Each compute node is connected to gateway switches, the switches that the compute nodes use must have a VLAN created on them.

> **Note:** Administrative IP is the IP Address of the compute node as configured on the management LAN at the time of commissioning.
>
> The External IP address is the static IP address that you assign to the EoIB interface.

To determine which switches are connected to the compute nodes:

1. Login to the compute node you wish to expose using the root user.

   For example:

   ```
   ssh root@IAMHOST1
   ```

2. Retrieve information about the active links on the InfiniBand framework using the following command:

   ```
   iblinkinfo.pl -R | grep hostname
   ```

   For example:

   ```
   # iblinkinfo.pl -R | grep IAMHOST1

   65   15[  ] ==( 4X 10.0 Gbps Active/  LinkUp)==>    121 2[  ] "el01cn01 EL-C
   192.168.10.3 HCA-1" (Could be 5.0 Gbps)
   64   15[  ] ==( 4X 10.0 Gbps Active/  LinkUp)==>    120 1[  ] "el01cn01 EL-C
   192.168.10.3 HCA-1" (Could be 5.0 Gbps)
   ```

   The first column shows the lid id of each of the gateway switches used. In this example, these are lids `65` and `64`. The number after the `==>` symbol shows the Infiniband Port Base Lid: Make a note of these in Table 5–4, " VNIC Worksheet".

3. Using the `ibswitches` command, determine the names of the gateway switches to which the compute node is connected.

   ```
   #ibswitches

   Switch  : 0x002128548042c0a0 ports 36 "SUN IB QDR GW switch el01gw03" enhanced
   port 0 lid 63 lmc 0
   Switch  : 0x002128547f22c0a0 ports 36 "SUN IB QDR GW switch el01gw02" enhanced
   port 0 lid 6 lmc 0
   Switch  : 0x00212856d0a2c0a0 ports 36 "SUN IB QDR GW switch el01gw04" enhanced
   port 0 lid 65 lmc 0
   Switch  : 0x00212856d162c0a0 ports 36 "SUN IB QDR GW switch el01gw05" enhanced
   port 0 lid 64 lmc 0
   ```

   The example output shows that:

   - `lid 64` is associated with gateway switch `el01gw05`.
   - `lid 65` is associated with gateway switch `el01gw04`.

   The GUID of the switch is the last 16 characters value after the `:`. For example, the GUID of Switch `el101gw04` is `00212856d0a2c0a0`.

   These are the gateway switches that must have a VLAN and VNICs defined. Make a note of these values in the Table 5–4, " VNIC Worksheet".

4. Retrieve information about the InfiniBand configuration using the `ibstat` command.

   ```
   # ibstat

   CA 'mlx4_0'
        CA type: MT26428
        Number of ports: 2
        Firmware version: 2.7.8100
        Hardware version: b0
        Node GUID: 0x0021280001a0a364
        System image GUID: 0x0021280001a0a367
   ```

```
Port 1:
     State: Active
     Physical state: LinkUp
     Rate: 40
     Base lid: 120
     LMC: 0
     SM lid: 6
     Capability mask: 0x02510868
     Port GUID: 0x0021280001a0a365
     Link layer: IB
Port 2:
     State: Active
     Physical state: LinkUp
     Rate: 40
     Base lid: 121
     LMC: 0
     SM lid: 6
     Capability mask: 0x02510868
     Port GUID: 0x0021280001a0a366
     Link layer: IB
```

The output shows that the compute node is connected to 2 InfiniBand switches, one for each port. The Base Lid links to the value you obtained in Step 2 above.

The `ibstat` command above shows that this compute node has two ports. Each of these ports is associated with a different switch.

Use the base lid to determine the switch to which each port is connected, by comparing the base lid with the output of the `iblinkinfo` command in Step 2. In our example, port 1 has a base lid of 120, which is associated with the switch with a lid of 64. You can now determine the actual switch name by looking at the output of the command `ibswitches` in step 3. In this example, this would be switch `el101gw05`.

To summarize, on this compute node, Port Number 1, which has a GUID of `0x0021280001a0a365` is connected to the switch `el101gw05` whose lid id is `64`.

Make a note of the last 16 characters of each GUID in Table 5–4, " VNIC Worksheet".

You now have the information about the existing networking.

5. Determine the unique MAC address for each of the VNICs you are going to create.

   The MAC address can be derived using the information in the worksheet using the following calculation:

   - The last three octets of the Switch GUID, plus the last three octets of the Internal IP address in hex. For example, the GUID of the switch `el101gw04` is `00212856d0a2c0a0`. The last three octets are: `a2c0a0`.
   - Separate each octet with a colon (:), for example, `a2:c0:a0`.
   - The internal (bond0) IP address of the Compute Node IAMHOST1 is: `192.168.10.1`
   - The last three octets are: `168.10.1`. Converted to Hexadecimal and separated by a colon: `a8:0a:01`

   Therefore, you can derive the MAC address as: `a2:c0:a0:a8:0a:01`

   Make a note of the MAC address in the worksheet.

6. Determine the switch upload connector.

a. Log in to one of the switches as root.

For example:

```
ssh root@el101gw05
```

b. At the command prompt, run the following:

```
listlinkup | grep Bridge

Bridge-0 Port 0A-ETH-1 (Bridge-0-2) up (Enabled)
Bridge-0 Port 0A-ETH-2 (Bridge-0-2) down (Enabled)
Bridge-0 Port 0A-ETH-3 (Bridge-0-1) down (Enabled)
Bridge-0 Port 0A-ETH-4 (Bridge-0-1) down (Enabled)
Bridge-1 Port 1A-ETH-1 (Bridge-1-2) down (Enabled)
Bridge-1 Port 1A-ETH-2 (Bridge-1-2) down (Enabled)
Bridge-1 Port 1A-ETH-3 (Bridge-1-1) down (Enabled)
Bridge-1 Port 1A-ETH-4 (Bridge-1-1) down (Enabled)
```

Identify the uplinks which can be used in the gateway. Any uplink that has a value of `up` can be used. In the example output, only `OA-ETH-1` is available for use.

Using the examples above, the worksheet entries for IAMHOST1 would look as follows:

Table 5–5 Example Worksheet for IAMHOST1

Compute Node	Administrative /External IP Address	Base Lid	GUID	Switch Lid	Switch Name	Connector	Switch GUID	MAC Address
IAMHOST1	10.168.10.1/10.10.10.1	120	0021280001a0a365	64	el01gw05	0A-ETH-1	00212856d162c0a0	62:C0:A0:A8:0A:01
		121	0021280001a0a366	65	el01gw04	0A-ETH-1	00212856d0a2c0a0	A2:C0:A0:A8:0A:01

7. Log in to the InfiniBand switch where master Subnet Manager is running. For more information, refer to the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

8. Run the following command to start the configuration process:

```
smpartition start
```

9. Run the following command to create a myEoIB partition with the pkey 0x005 with a full membership:

```
smpartition create -n myEoIB -pkey 0x005 -m full
```

10. Use the following command to add the compute node port GUIDs to the IB partition defined by partition key created previously. Use this partition key while creating the VLAN as described in Section 5.5.3.

```
smpartition add -pkey pkey -port compute_node_port_GUID -m both
```

Where `pkey` is the partition key of the IB partition created in this step. Use this pkey when creating the VLAN.

`compute_node_port_GUID` is the GUID value from the worksheet.

11. Run the following command to view the changed partition configuration:

    ```
    smpartition list modified
    ```

    This command displays the new partition with its pkey, ports added to the partition, and membership type.

12. Run the following command to confirm the partition configuration:

    ```
    smpartition commit
    ```

5.5.3 Step 2 - Create a Virtual LAN

Create a virtual LAN on each of these switches using the following steps:

1. Log in to the gateway switch that you stored in the worksheet, for example, `el01g04`, as the user `ilom-admin`.

    For example:

    ```
    ssh ilom-admin@el01gw04
    ```

2. Change to the system management framework by entering the following:

    ```
    cd /SYS/Fabric_Mgmt
    ```

    For example:

    ```
    Oracle(R) Integrated Lights Out Manager

    Version ILOM 3.0 r47111

    Copyright (c) 2010, Oracle and/or its affiliates. All rights reserved.
    -> cd /SYS/Fabric_Mgmt
    ```

3. Launch a restrict shell by entering the `show` command:

    ```
    show
    ```

4. Run the following command to associate a connector with the VLAN that will be used:

    ```
    createvlan connector -vlan 0 -pkey default
    ```

    Where:

    `connector` is the name of the switch interface from the worksheet.

    `vlan` is the number of the Virtual Lan.

    `pkey` is the partition key.

5. Verify the virtual LAN is working using the following command:

    ```
    showvlan
    ```

    Expected output:

    ```
     Connector/LAG VLN PKEY
        ----------- ---- ----
         0A-ETH-1   125 ffff
         0A-ETH-1     0 ffff
    ```

6. Repeat once for each switch in the VNIC worksheet.

5.5.4 Step 3 - Create Virtual Network Cards

Create a virtual network card on the switch to allow compute nodes to recognize it as a network card it can use for communication.

You need to create a VNIC for each port on each switch attached to each externally facing compute node. Refer to Table 5–4, " VNIC Worksheet" for details.

To create a VNIC:

1. Login to the gateway switch you stored in the worksheet, for example, `el01g04` as the user `ilom-admin`.

   For example:

   ```
   ssh ilom-admin@el01gw04
   ```

2. Change to the system management framework by entering the following:

   ```
   cd /SYS/Fabric_Mgmt
   ```

   For example:

   ```
   Version ILOM 3.0 r47111

   Copyright (c) 2010, Oracle and/or its affiliates. All rights reserved.
   -> cd /SYS/Fabric_Mgmt
   ```

3. Launch a restrict shell by entering the `show` command:

   ```
   show
   ```

4. Run the following command to a VNIC:

   ```
   createvnic connector -guid compute_node_port_GUID -mac unique_mac_address -pkey
   default -vlan 0
   ```

   Where `connector` is the **Connector** column in the worksheet.

   `compute_node_port_GUID` is the **GUID** column in the worksheet.

   `unique_mac_address` is the **MAC Address** in the worksheet.

   `pkey` and `vlan` are the values you used when you created the VLAN in Section 5.5.3, "Step 2 - Create a Virtual LAN."

   For example:

   ```
   createvnic 0A-ETH-1 -guid 0021280001a0a366 -mac A2:C0:A0:A8:0A:01 -pkey default
   -vlan 0
   ```

5. Verify that the VNIC has been created properly by running the following command:

   ```
   showvnics
   ```

   Example output:

   ```
   ID  STATE    FLG IOA_GUID                NODE                             IID
   MAC               VLN PKEY GW
   --- -------- --- ----------------------- -------------------------------- ----
   ----------------- --- ---- --------
   94  UP       N   0021280001EFA4BF        el01cn01EL-C 192.168.10.1        0000
   A2:C0:A0:A8:0A:01 0   ffff 0A-ETH-1
   ```

Look for the MAC address of the card created and verify that its status is shown as `up`.

6. If the VNIC is up, repeat Steps 1-5 to add a VNIC to the next interface. If the VNIC is in a WAIT state, follow Steps 7-9 to ensure the Port GUID has been added to the Pkey.

7. Log onto the master switch. This can be obtained by issuing the following command at any switch:

```
getmaster
```

8. Log back on to the switch from Step 5 and confirm the VNIC is now up:

```
showvnics
```

9. Repeat all the steps, starting with Step 1, to create each of the necessary VNCs.

5.5.5 Step 4 - Configure Compute Node Networking and Assign Physical IP Address

Define a new bonded network interface on the compute node that exposes the vNICs you just created as a single interface to applications, so that the compute node can be accessed using a fixed IP by an external load balancer. Each compute node has two Virtual Network Interface Cards created.

To make configuring the network easier you can use the following worksheet:

Table 5–6 VNIC Worksheet

Compute Node	EoIB IP Address	Netmask	Interface	Network Device	MAC Address	EPORT_ID	IOA_PORT	Interface Device Name	Interface File
IAMHOST1									
IAMHOST2									

To configure the network:

1. Log in to the compute node as the root user.

   For example:

   ```
   ssh root@IAMHOST1
   ```

2. On the compute node, run the following command to display the list of VNICs available:

   ```
   mlx4_vnic_info -i
   ```

   This command returns the details of the virtual network cards. Make a note of the following in the worksheet:

   - `Network Device`
   - `MAC Address`

- `EPORT_ID`
- The number following the colon (:) of the `IOA_PORT`.

3. Create interface files for the VNICs on the compute node.

   To ensure correct failover behavior, the name of the VNIC interface file and the value of the DEVICE directive in the interface file must not be based on the kernel-assigned `ethX` interface name (`eth4`, `eth5`, and so on). Instead, Oracle recommends that the interface file name and value of the `DEVICE` directive in the interface file be derived from the `EPORT_ID` and `IOA_PORT` values:

   Note: Any other unique naming scheme is also acceptable.

   a. Determine the interface device name using the following convention:

   ```
   ethEPORT_IOA_PORT
   ```

   For example:

   ```
   eth331_1
   ```

   Make a note of the interface device name in the worksheet.

   b. Determine the interface file name using the following convention:

   ```
   ifcfg-DeviceName
   ```

   For example:

   ```
   ifcfg-eth331_1
   ```

   Make a note of the interface file name in the worksheet.

   Using the examples above for IAMHOST1, the worksheet entry would look as follows:

Table 5–7 VNIC Worksheet

Compute Node	EoIB IP Address	Netmask	Interface	Network Device	MAC Address	EPORT_ID	IOA_PORT	Interface Device Name	Interface File
IAMHOST1	10.10.10.1	255.255.224.0	bond1	eth4	A2:C0:A0:A8:0A:03	331	1	eth331_1	ifcfg-eth331_1
				eth5	62:C0:A0:A8:0A:03	331	2	eth331_2	ifcfg-eth331_2

Note: Table 5–1 Exalogic Physical IP Addresses Worksheet, shows the interface (Bond name) for various types of communication. The interface for compute nodes to be accessed by external load balancer using a fixed IP is Bond1.

The MAC address is the value of the MAC address generated in the VNICs worksheet.

c. Create the interface file for the first VNIC, eth4 in the example, by using a text editor, such as VI, and save the file in the following directory:

```
/etc/sysconfig/network-scripts
```

Name the file ifcfg-eth331_1 (from the worksheet).

This file will have the following contents:

```
DEVICE=eth331_1
BOOTPROTO=none
ONBOOT=yes
HWADDR=a2:c0:a0:a8:0A:03
MASTER=bond1
SLAVE=yes
MTU=1500
```

Where:

DEVICE the **Derived Name** in the worksheet.

HWADDR is the **Mac Address** in the worksheet.

d. Create a second interface file for the remaining network card.

e. Create a bonded Ethernet Card encompassing each of the network devices by creating a file named ifcfg-*Interface*, for example:

```
ifcfg-bond1
```

The file will have the following contents:

```
DEVICE=bond1
IPADDR=10.10.10.1
NETMASK=255.255.224.0
BOOTPROTO=none
USERCTL=no
TYPE=Ethernet
ONBOOT=yes
IPV6INIT=no
BONDING_OPTS="mode=active-backup miimon=100 downdelay=5000 updelay=5000"
GATEWAY=10.10.18.1
MTU=1500
```

Where:

Device is the Interface Name.

IPADDR is the external IP address being assigned.

NETMASK is the netmask of the IP Address.

GATEWAY is the IP address of your gateway.

f. Restart networking using the following command:

```
service network restart
```

5.6 Routing for Multi-Homed Hosts

Now that you have added new interfaces to each Host, having only one default gateway might not be sufficient. You might want to have one interface for an Internet connection and another for a corporate WAN, for example.

In the example below, the different interfaces are shown, along with example IP addresses and gateway requirements:

Interface	IP Address	Gateway Requirements
eth0	201.19.23.128 / 24	Gateway IP 201.19.23.1
bond0	192.168.10.1 / 24	No Gateway requirements
bond1	10.10.10.101/ 24	Gateway IP 10.10.10.1

As you can see, eth0 and bond1 must have their own respective default gateways.

Bond0, however, does not have any default gateway requirements. It is simply confined to their actual Layer 3 subnet.

To get around this, create rules and tables for routing lookups, as follows.

1. Check the existing table IDs by issuing this command:

   ```
   ip rule list
   ```

2. Choose a unique id that has NOT already been used. In this example, we'll use 224 and 225.
3. For eth0, create the following two files:

   The file `/etc/sysconfig/network-scripts/rule-eth0`, which contains:

   ```
   from 201.19.23.128/32 table 224
   to 201.19.23.128 table 224
   ```

   The file `/etc/sysconfig/network-scripts/route-eth0`, which contains:

   ```
   201.19.23.0/24 dev eth0 table 224
   default via 201.19.23.1 dev eth0 table 224
   ```

4. For bond1 create the following two files:

   The file /etc/sysconfig/network-scripts/rule-bond1, which contains:

   ```
   from 10.10.10.10/32 table 225
   to 10.10.10.10 table 225
   ```

   The file /etc/sysconfig/network-scripts/route-bond1, which contains:

   ```
   10.10.10.0/24 dev bond1 table 225
   default via 10.10.10.1 dev bond1 table 225
   ```

5. Restart the network to make the configuration effective.

   ```
   service network restart
   ```

   The hosts are now accessible from both routers.

5.7 Enable Virtual IP Addresses

Having completed the network chapter you need to assign virtual IP addresses to the various network interfaces and hosts as described in link to Section 9.8, "Enabling Virtual IP Addresses."

5.8 Adjust MTU (maximum transmission units) Value for IPoIB Interface bond0

When the Exalogic rack is commissioned, it sets up the networking configuration for the internal IPoIB interface bond0. Changed the MTU value created to the value 6400 for improved performance.

To change the value, edit the `ifcfg-bond0` file located in the following director:

```
/etc/sysconfig/network-scripts
```

Change the value of `MTU` to 64000. The following example is an ifcfg-bond0 file after editing the MTU value:

```
######## DO NOT EDIT THIS FILE ########
######## GENERATED BY EXALOGIC ########
DEVICE=bond0
IPADDR=192.168.47.67
NETMASK=255.255.240.0
BOOTPROTO=none
USERCTL=no
TYPE=Ethernet
ONBOOT=yes
IPV6INIT=no
BONDING_OPTS="mode=active-backup miimon=100 downdelay=5000 updelay=5000"
MTU=64000
```

Save the file and restart the networking using the command service network restart.

> **See Also:** For the latest recommended values see MOS note: Revised MTU Tuning Recommendations for the IPoIB Related Network Interfaces on Exalogic Physical and Virtual Environments (Doc ID 1624434.1), which is available on My Oracle Support at `https://support.oracle.com/`.

5.9 Enable Multicast for bond0

Even though WebLogic clusters are configured to use unicast for cluster communications, Oracle Identity Manager has an internal dependency on multicast. For that reason, you must enable multicast on the IPoIB network.

You enable multicast by creating a file called `route-bond0` in the directory `/etc/sysconfig/network-scripts`.

This file must have the following contents:

```
224.0.0.0/4 dev bond0
```

After creating the file, restart the network by executing the command

```
service network restart
```

5.10 Verifying Network Connectivity

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

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

```
ping -I interface hostname
```

for example

```
ping -I bond1 IADADMINVHN
```

Perform this test for each entry in Table 5–1, " Exalogic Physical IP Addresses Worksheet" and Table 6–2, " Exalogic Virtual IP Addresses Worksheet", depending on your deployment type.

```
ping -I bond1 IADADMINVHN
ping -I bond0 SOAHOST1VHN
ping -I bond0 SOAHOST2VHN
ping -I bond0 OIMHOST1VHN
ping -I bond0 OIMHOST2VHN
ping -I bond0 IAMHOST1
ping -I bond0 IAMHOST2
ping -I bond1 IAMHOST1EXT
ping -I bond1 IAMHOST2ext
ping -I bond1 OTDADMINVHN
ping -I bond1 DBHOST1
ping -I bond1 DBHOST2
ping -I bond1 IAMDBSCAN
```

In addition, test that the compute nodes allow access to the database servers by pinging the database hosts and the Gridlink scan address. For example

```
ping -I bond1 DBHOST1
ping -I bond1 DBHOST2
ping -I bond1 IAMDBSCAN
```

5.11 Verifying Multicast Connectivity

Oracle provides a simple command to test that multicast is configured and working correctly. However, this command is available only after the Oracle software has been installed.

Use the following command to verify multicast after provisioning has been completed:

```
set JAVA_HOME to JAVA_HOME
```

Change the directory to the following:

```
IGD_ORACLE_HOME/coherence_3.7/bin
```

Run the following command:

```
multicast-test.sh -ttl 0 -local oimhost1
```

Where `oimhost1` is the name of the host associated with the network interface `bond0`.

Run the command on each of the `oimhosts` to perform a multicast test.

For details about the `multicast-test.sh` program, see "Performing a Multicast Connectivity Test" in the *Oracle Coherence Administrator's Guide*.

6

Configuring Exalogic Networking for a Virtual Environment

This chapter describes virtual Exalogic networking.

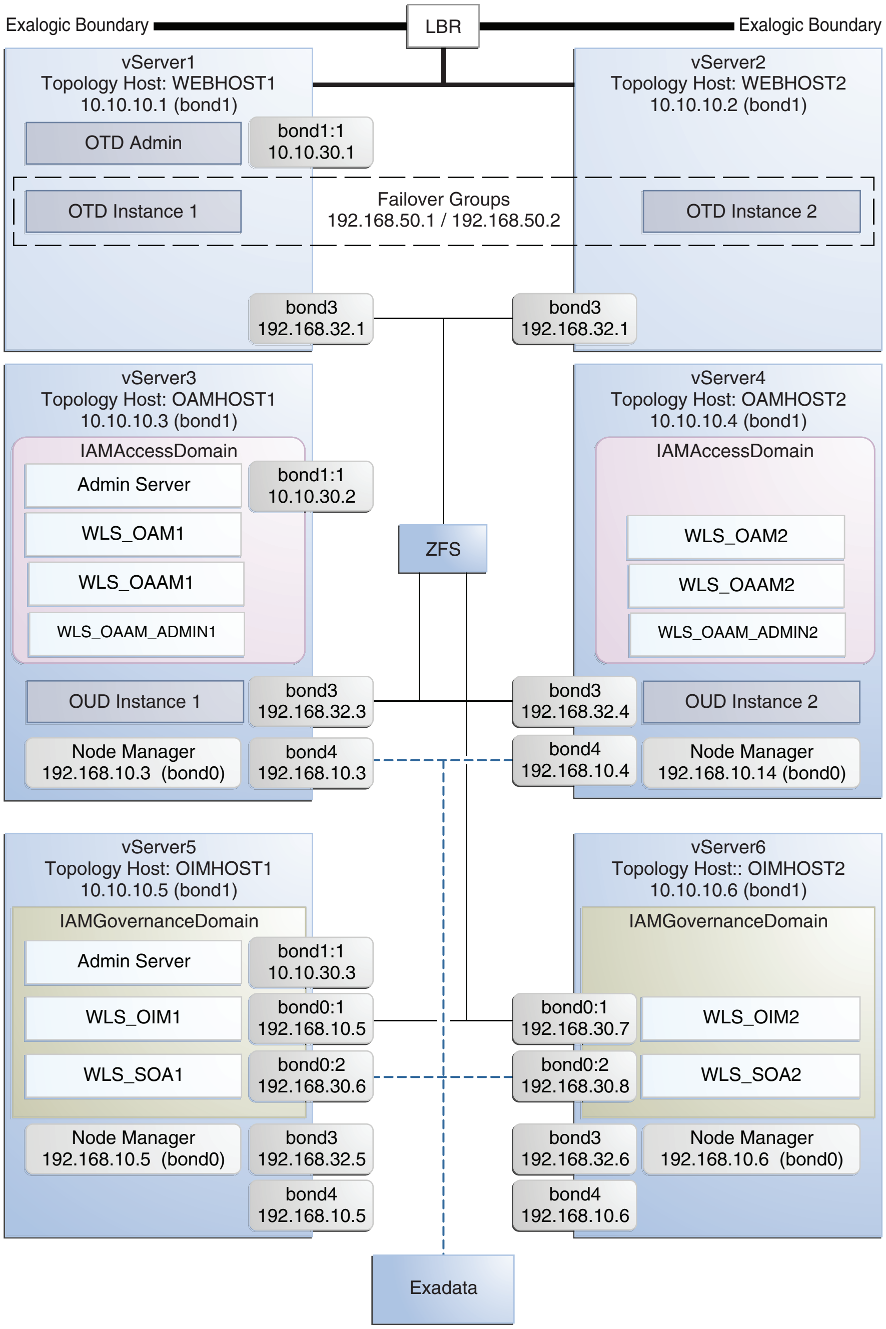
The contents in this chapter are specific to the Exalogic virtual environment and should be read in conjunction with the Chapter 4, "Networking Overview."

This chapter contains the following sections:

- Section 6.1, "Network Map"
- Section 6.2, "Explanation of Network Interfaces Map"
- Section 6.3, "Host Name and Networking Overview"
- Section 6.4, "Preparing the Network on Virtual Exalogic"

6.1 Network Map

Figure 6–1 Virtual Exalogic Network Map



6.2 Explanation of Network Interfaces Map

In a Virtual Exalogic deployment, A hardware load balancer is used to distribute requests to two vServers in the Exalogic Rack which host Oracle Traffic Director. The Oracle Traffic director instances then direct traffic to other vServers which host the Identity and Access Management components.

The diagram above shows how these vServers are networked together and to the external corporate network where the load balancer sits.

This section contains the following topics:

- Section 6.2.2, "Network Interface Bonding"
- Section 6.2.5.2, "Virtual Server 2 (vServer2)"
- Section 6.2.5.3, "Virtual Server 3 (vServer3)"
- Section 6.2.5.4, "Virtual Server 4 (vServer4)"
- Section 6.2.6, "Virtual Server 5 (vServer5)"
- Section 6.2.6.1, "Virtual Server 6 (vServer6)"

6.2.1 Load Balancer

An external load balancer sits outside of the exalogic machine rack. Its purpose is to receive requests on the public ethernet network and distribute those requests to the Oracle Traffic Director nodes inside the machine rack using the front end EoIB network or to the external Oracle HTTP Servers.

6.2.2 Network Interface Bonding

In Virtual Exalogic Deployments, these are assigned when the vServer is created. Therefore, the exact bonding is determined by the order the networks are attached to the vServer.

For the purposes of this document, assume the network interfaces are as follows:

Table 6–1 Network Interfaces

Purpose	Network	Interface
Management Network	EoIB	eth0
Private Internal Network	IPoIB	bond0
Client Access Network	EoIB	bond1
Internal Administration Network	IPoIB	bond2 (not used)
Internal Storage Network	IPoIB	bond3
Exadata Network	IPoIB	bond4

6.2.3 Oracle Traffic Director

Oracle Traffic Director (OTD) serves two functions: load balancing, and HTTP server.

As a load balancer, Oracle Traffic Director is configured in a way that it can direct requests to the Oracle Unified Directory servers using the internal IPoIB network using TCP and to direct internal call back requests from Oracle Traffic Director to SOA servers using the internal IPoIB network using HTTP.

Unless External Oracle HTTP Servers are used, then Oracle Traffic Director also functions as an HTTP Server. Oracle Traffic Director listens on the front end EoIB network for HTTP requests originating from the external load balancers. If these requests require access to the WebLogic managed servers on the compute nodes, then it directs these requests accordingly using the internal IPoIB network. *HTTP* requests on the front-end EoIB network.

6.2.4 External Oracle HTTP Servers

Optionally, you can use Oracle HTTP Servers, which sit on servers outside of the Exalogic machine rack. These servers receive requests from the Load Balancer and distribute those requests to application compute nodes inside the machine rack using EoIB.

6.2.5 Virtual Servers

In an Exalogic Virtual deployment, virtual servers are used instead of physical compute nodes to host services. These virtual hosts look and feel like physical servers but they are actually virtual environments managed by Exalogic Control.

These are referred to as vServers.

The following sections describe the networking configuration of each of the vServers.

6.2.5.1 Virtual Server 1 (vServer1)

vServer1 (WEBHOST1) hosts Oracle Traffic director which acts as both an internal load balancer and a web server.

- It is configured to use the EoIB client access network. It uses this network to communicate with the external load balancer.
- It is configured to use the IPoIB network for internal communications.
- Oracle Traffic Director enables an IP address using a failover group to route requests to the Oracle Unified Directory servers using the IPoIB network.
- Oracle Traffic Director acts as a failover node in the event that the IP address used for internal callbacks fails.
- Oracle Traffic Directory is used to route application requests to the Weblogic managed servers making up the Application Tier.

6.2.5.2 Virtual Server 2 (vServer2)

vServer2 (WEBHOST2) serves two purposes. It hosts Oracle Traffic director which acts as both an internal load balancer and a web server. It also hosts the Oracle Identity and Access Management Applications which comprise Access Manager, Oracle Identity Manager and Oracle Unified Directory.

- It is configured to use the EoIB client access network. It uses this network to communicate with the external load balancer.
- It is configured to use the IPoIB network for internal communications.
- Oracle Traffic Director enables an IP address using a failover group to route internal callback requests to SOA servers using the IPoIB network.
- Oracle Traffic Director acts as a failover node in the event that the IP address used for Oracle Unified Directory fails.
- Oracle Traffic Directory is used to route application requests to the Weblogic managed servers making up the Application Tier.

6.2.5.3 Virtual Server 3 (vServer3)

vServer3 (OAMHOST1) hosts the Oracle Identity and Access Management Applications which support the IAMAccessDomain and comprise Access Manager and Oracle Unified Directory.

- It can be configured to use the EoIB client access network. It uses this network to communicate with external database servers or for external Oracle HTTP servers to communicate with the Weblogic Managed Servers.
- It is configured to use the IPoIB network for internal communications.
- Weblogic Managed Servers receive requests from Oracle Traffic Director on the internal IPoIB network.
- Node Manager, which is used to start and stop the WebLogic managed servers, is configured to accept requests on the internal IPoIB interface.
- This node hosts a virtual (floating) IP address which is configured on the client access network. This virtual IP addresses is used by the administration server. Although not necessary to use the client access network. The benefit of doing so is that it is possible to monitor the administration server outside of the Exalogic machine.
- Oracle Unified Directory listens for requests on the internal IPoIB network.

6.2.5.4 Virtual Server 4 (vServer4)

vServer4 (OAMHOST2) hosts the Oracle Identity and Access Management Applications which support the IAMAccessDomain and comprise Access Manager and Oracle Unified Directory.

- It can be configured to use the EoIB client access network. It uses this network to communicate with external database servers or for external Oracle HTTP servers to communicate with the Weblogic Managed Servers.
- It is configured to use the IPoIB network for internal communications.
- Weblogic Managed Servers receive requests from Oracle Traffic Director on the internal IPoIB network.
- Node Manager, which is used to start and stop the WebLogic managed servers is configured to accept requests on the internal IPoIB interface.
- Oracle Unified Directory listens for requests on the internal IPoIB network.

6.2.6 Virtual Server 5 (vServer5)

vServer5 (OIMHOST1) hosts the Oracle Identity and Access Management Applications which comprise the IAMGovernanceDomain, namely Oracle Identity Manager.

- It can be configured to use the EoIB client access network. It uses this network to communicate with external database servers or for external Oracle HTTP servers to communicate with the Weblogic Managed Servers.
- It is configured to use the IPoIB network for internal communications.
- Weblogic Managed Servers receive requests from Oracle Traffic Director on the internal IPoIB network.
- Node Manager, which is used to start and stop the WebLogic managed servers is configured to accept requests on the internal IPoIB interface.
- This node hosts a virtual (floating) IP address which is configured on the client access network. This virtual IP addresses is used by the administration server. Although not necessary to use the client access network. The benefit of doing so is that it is possible to monitor the administration server outside of the Exalogic machine.

- Two virtual (floating) IP addresses are attached to the IPoIB interface, which are used by the Oracle Identity Manager and SOA managed servers to facilitate server migration.

6.2.6.1 Virtual Server 6 (vServer6)

vServer6 (OIMHOST2) hosts the Oracle Identity and Access Management Applications which comprise the IAMGovernanceDomain, namely Oracle Identity Manager.

- It can be configured to use the EoIB client access network. It uses this network to communicate with external database servers or for external Oracle HTTP servers to communicate with the Weblogic Managed Servers.
- It is configured to use the IPoIB network for internal communications.
- Weblogic Managed Servers receive requests from Oracle Traffic Director on the internal IPoIB network.
- Node Manager, which is used to start and stop the WebLogic managed servers is configured to accept requests on the internal IPoIB interface.
- Two virtual (floating) IP addresses are attached to the IPoIB interface, which are used by the Oracle Identity Manager and SOA managed servers to facilitate server migration.

6.3 Host Name and Networking Overview

Networking is a complicated but critical part of any Exalogic deployment. This guide utilizes the IPoIB network for internal communications and the EoIB network for external communications.

Table 6–2, " Exalogic Virtual IP Addresses Worksheet" is a summary of the required networking setup in the Exalogic machine rack. The following sections describe in detail how to set up this networking.

A column has been added to the table to allow you to add your own values for easier cross referencing.

Appropriate host name resolution is critical to topology designs that can sustain network changes, system relocation and disaster recovery scenarios. It is important that the required DNS (either `/etc/hosts` or central DNS server) definitions are in place and that WebLogic Servers use host names and virtual host names instead of using IP addresses and virtual IP addresses directly. Additionally, the Exalogic enterprise deployment requires a set of virtual server names for routing requests to the proper server or service within the topology through the external load balancer and the Oracle Traffic Director servers. See Section 4.3, "Virtual Server Names Used by the Topology."

These virtual server names must be resolvable in the corporate network. IPoIB addresses must be resolved only inside the rack's name resolution system. If multiple racks are going to be connected, to elude possible IP conflict, it is good practice to place these also in a central DNS server. Network administrators at the corporate level should enable this. Alternatively host names may be resolved through appropriate `/etc/hosts` file propagated through the different nodes. Table 6–2, " Exalogic Virtual IP Addresses Worksheet" provides an example of names for the different floating IP addresses used by servers in the SOA system.

Table 6–2 Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
WEBHOST1	bond0	192.168.10.1/255.255.224.0		IPoIB/ Fixed	vServer1/WEBHOST1	NA	Access to vServer11/WEB OST1 via the internal IPoIB network.
WEBHOST2	bond0	192.168.10.2/255.255.224.0		IPoIB/ Fixed	vServer2/WEBHOST2	NA	Access to vServer2/WEBH ST2 via the internal IPoIB network.
OAMHOST1	bond0	192.168.10.3/255.255.224.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	Access to vServer3/OAM OST1 via the internal IPoIB network
OAMHOST2	bond0	192.168.10.4/255.255.224.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	Access to vServer4/OAM OST2 via the internal IPoIB network
OIMHOST1	bond0	192.168.10.5/255.255.224.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	Access to vServer5/OIMH ST1 via the internal IPoIB network
OIMHOST2	bond0	192.168.10.6/255.255.224.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	Access to vServer6/OIMH ST2 via the internal IPoIB network
OTDADMINVHN	bond1:1	10.10.30.1/255.255.224.0		EoIB /Floating	vServer1/WEBHOST1	OTD Administration Server	A floating IP address for the Administration Server is recommended, i you want to manually migrat the OTD Administration Server from WEBHOST1 to WEBHOST2.
IADADMINVHN	bond1:2	10.10.30.2/255.255.224.0		EoIB /Floating	vServer3/OAMHOST1	IAMAccessDomain Administration Server	A floating IP address for the IAMAccessDom n Administratio Server is recommended, i you want to manually migrat the Administrati Server from OAMHOST1 to OAMHOST2.

Table 6–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
IGDADMIN VHN	bond1:3	10.10.30.3/255.255.224.0		EoIB /Floating	vServer5/OIMHOST1	IAMGovernanceDomain Administration Server	A floating IP address for the IAMGovernanceDomain Administration Server is recommended, if you want to manually migrate the Administration Server from OIMHOST2 to OIMHOST1
WEBHOST1 VHN1	OTD	10.10.50.1/255.255.224.0		EoIB /Floating	vServer1/WEBHOST1	OTD - WEBHOST1	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect. This is optional
WEBHOST2 VHN1	OTD	10.10.50.2/255.255.224.0		EoIB /Floating	vServer2/WEBHOST2	OTD - WEBHOST2	A floating IP Address managed by OTD. This is the IP Address to which load balancers will connect.
OIMHOST1 VHN	bond0:1	192.168.30.1/255.255.240.0		IPoIB/ Floating	vServer5/OIMHOST1	WLS_OIM1 Default Channel	Initially enabled in OIMHOST1 and can be failed over by server migration to OIMHOST2
OIMHOST2 VHN	bond0:1	192.168.30.2/255.255.240.0		IPoIB/ Floating	vServer6/OIMHOST2	WLS_OIM2 Default Channel	Initially enabled in OIMHOST2 and can be failed over by server migration to OIMHOST1
SOAHOST1 VHN	bond0:2	192.168.30.3/255.255.240.0		IPoIB/ Floating	vServer5/OIMHOST1	WLS_SOA1 default channel	Initially enabled in OIMHOST1 and can be failed over by server migration to OIMHOST2
SOAHOST2 VHN	bond0:2	192.168.30.4/255.255.240.0		IPoIB/ Floating	vServer6/OIMHOST2	WLS_SOA2 default channel	Initially enabled in OIMHOST2 and can be failed over by server migration to OIMHOST1.

Table 6–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
WEBHOST1-EXT	bond1	10.10.10.1/255.255.240.0		EoIB/Fixed	vServer1/WEBHOST1	NA	A fixed IP allowing the vServer to be accessed by an External Load balancer
WEBHOST2-EXT	bond1	10.10.10.2/255.255.240.0		EoIB/Fixed	vServer2/WEBHOST2	NA	A fixed IP allowing the vServer to be accessed by an External Load balancer
WEBHOST1-STOR	bond3	192.168.32.1/255.255.240.0		IPoIB/Fixed	vServer1/WEBHOST1	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.
WEBHOST2-STOR	bond3	192.168.32.2/255.255.240.0		IPoIB/Fixed	vServer2/WEBHOST2	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.
OAMHOST1-STOR	bond3	192.168.32.3/255.255.240.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.
OAMHOST2-STOR	bond3	192.168.32.4/255.255.240.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.
OIMHOST1-STOR	bond3	192.168.32.5/255.255.240.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.
OIMHOST2-STOR	bond3	192.168.32.6/255.255.240.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	A fixed IP addre allowing the vServer to conne to the ZFS Storag appliance using the internal network.

Table 6–2 (Cont.) Exalogic Virtual IP Addresses Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OAMHOST1-DATA	bond4	192.168.10.3/255.255.240.0		IPoIB/Fixed	vServer3/OAMHOST1	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OAMHOST2-DATA	bond3	192.168.10.4/255.255.240.0		IPoIB/Fixed	vServer4/OAMHOST2	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OIMHOST1-DATA	bond4	192.168.10.5/255.255.240.0		IPoIB/Fixed	vServer5/OIMHOST1	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
OIMHOST2-DATA	bond3	192.168.10.6/255.255.240.0		IPoIB/Fixed	vServer6/OIMHOST2	NA	A fixed IP address allowing the vServer to connect to the Exadata appliance using the default internal network.
IDMINTERNAL	OTD	192.168.50.1/255.255.224.0		IPoIB/ Floating	vServer1/WEBHOST1	NA	Oracle Traffic Director failover group for SOA
IDSTORE	OTD	192.168.50.2/255.255.224.0		IPoIB/ Floating	vServer2/WEBHOST2	NA	Oracle Traffic Director failover group for Oracle Unified Directory

6.3.1 Additional Requirements for External OHS

If External OHS Servers are being used then the additional host names in the following table apply to an Exalogic Virtual configuration.

Table 6–3 Exalogic Virtual OHS Configuration Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OHSHOST1	eth0	201.19.23.10/255.255.255.0		ETH0/Fixed	External OHSHOST1	Oracle HTTP Server	Fixed IP that Oracle HTTP Server Listens on
OHSHOST2	eth0	201.19.23.11/255.255.255.0		ETH0/Fixed	External OHSHOST2	Oracle HTTP Server	Fixed IP that Oracle HTTP Server Listens on

Table 6–3 (Cont.) Exalogic Virtual OHS Configuration Worksheet

Hostname Example for This Guide	Interface	IP Address /Subnet	Customer Value	Type	Host	Bound By	Details
OIMHOST1 VHN-EXT	bond1:2	10.10.10.7/255.255.224.0		EoIB/Floating	ComputeNode1/IAMHOST1/vServer5	WLS_OIM1 Default External Channel	Initially enabled on vServer5, can be failed over by server migration to vServer6
OIMHOST2 VHN-EXT	bond1:2	10.10.10.8/255.255.224.0		EoIB/Floating	ComputeNode2/IAMHOST2/vServer6	WLS_OIM2 Default External Channel	Initially enabled on vServer6, can be failed over by server migration to vServer5

6.4 Preparing the Network on Virtual Exalogic

This section contains the following topics:

- Section 6.4.1, "Public EoIB Client Access Network"
- Section 6.4.2, "Creating a Private IPoIB Network"
- Section 6.4.3, "Reserving Virtual IP Addresses"

6.4.1 Public EoIB Client Access Network

If you have not already done so, you must create a public client access network, which allows virtual servers to connect to the main organizational ethernet network. For details on how to do this refer to the Oracle Exalogic Elastic Cloud Administrator's Guide.

For the purposes of this Enterprise Deployment guide, it is assumed that this network has already been created and is called: EoIB-client

6.4.2 Creating a Private IPoIB Network

You need to create a private network to allow each of the vServers in the deployment to communicate with each other. This network will only be available to assigned vServers and ensures that network communication between IAM vServers is isolated from other network traffic.

To Create a Private IPoIB network for exclusive communication between the vServers in the deployment, perform the following steps:

1. Log in to Exalogic Control at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Expand **vDC Management**.
3. Then Navigate to **vDCs - Accounts - Cloud User Account**
4. In the Actions window, click **Create Private vNet**.
5. Enter a **Name** For example: `IPoIB_IAM`.
6. Click **Next**.
7. Select the **Number of IP Addresses** to reserve on the network.
8. Click **Next**.

9. Click **Finish**.

6.4.3 Reserving Virtual IP Addresses

In a virtual Exalogic deployment, if you wish to use IP addresses from the default pool, these IP addresses must be reserved on the Private IPoIB network created in the previous section. Reserving the IP addresses ensures that they are not automatically assigned elsewhere.

To reserve IP addresses perform the following steps:

1. Log in to Exalogic Control at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Expand **vDC Management**.
3. Then Navigate to **vDCs - Accounts - Cloud User Account**
4. Click the **Networks** tab. The Network Dashboard is displayed.
5. Select the network **IPoIB_IAM** listed under Private vNets
6. Click **Allocate VIP Addresses**. The Allocate VIP from vNet window is displayed.
7. Choose the number of virtual IP addresses you wish to reserve, for example 6, and click **Allocate VIP**. A window shows what virtual IP addresses have been reserved. Make a note of these.

Note: This is only for virtual IP addresses on the internal IPoIB network, you will need to allocate virtual IP Addresses on the client access network for communication with Oracle Traffic Director and the Administration Servers.

6.5 Routing for Multi-Homed Hosts

Now that you have added new interfaces to each Host, having only one default gateway might not be sufficient. You might want to have one interface for an Internet connection and another for a corporate WAN, for example.

In the example below, the different interfaces are shown, along with example IP addresses and gateway requirements:

Interface	IP Address	Gateway Requirements
eth0	201.19.23.128 / 24	Gateway IP 201.19.23.1
bond0	192.168.10.1 / 24	No Gateway requirements
bond1	10.10.10.101/ 24	Gateway IP 10.10.10.1

As you can see, eth0 and bond1 must have their own respective default gateways.

Bond0, however, does not have any default gateway requirements. It is simply confined to their actual Layer 3 subnet.

Note: These steps are shown here for completeness. However, the actions for updating the networking files must be performed once the vServers are created.

To get around this, create rules and tables for routing lookups, as follows.

1. Check the existing table IDs by issuing this command:

   ```
   ip rule list
   ```

2. Choose a unique id that has NOT already been used. In this example, we'll use 224 and 225.
3. For eth0, create the following two files:

   The file `/etc/sysconfig/network-scripts/rule-eth0`, which contains:

   ```
   from 201.19.23.128/32 table 224
   to 201.19.23.128 table 224
   ```

   The file `/etc/sysconfig/network-scripts/route-eth0`, which contains:

   ```
   201.19.23.0/24 dev eth0 table 224
   default via 201.19.23.1 dev eth0 table 224
   ```

4. For bond1 create the following two files:

   The file /etc/sysconfig/network-scripts/rule-bond1, which contains:

   ```
   from 10.10.10.10/32 table 225
   to 10.10.10.10 table 225
   ```

   The file /etc/sysconfig/network-scripts/route-bond1, which contains:

   ```
   10.10.10.0/24 dev bond1 table 225
   default via 10.10.10.1 dev bond1 table 225
   ```

5. Restart the network to make the configuration effective.

   ```
   # service network restart
   ```

   The hosts are now accessible from both routers.

6.6 Enable Virtual IP Addresses

Having completed the network chapter you need to assign virtual IP addresses to the various network interfaces and hosts as described in link to Section 9.8, "Enabling Virtual IP Addresses."

6.7 Verifying Network Connectivity

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

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

```
ping -I interface hostname
```

for example

```
ping -I bond1 IADADMINVHN
```

Perform this test for each entry in Table 5–1, " Exalogic Physical IP Addresses Worksheet" and Table 6–2, " Exalogic Virtual IP Addresses Worksheet", depending on your deployment type.

```
ping -I bond1 IADADMINVHN
```

```
ping -I bond0 SOAHOST1VHN
ping -I bond0 SOAHOST2VHN
ping -I bond0 OIMHOST1VHN
ping -I bond0 OIMHOST2VHN
ping -I bond0 OIMHOST1
ping -I bond0 OIMHOST2
ping -I bond0 OAMHOST1
ping -I bond0 OAMHOST2
ping -I bond0 WEBHOST1
ping -I bond0 WEBHOST2
ping -I bond1 IAMHOST1EXT
ping -I bond1 IAMHOST2ext
ping -I bond1 WEBHOST1ext
ping -I bond1 WEBHOST2ext
ping -I bond1 OTDADMINVHN
ping -I bond1 DBHOST1
ping -I bond1 DBHOST2
ping -I bond1 IAMDBSCAN
```

7 Preparing Storage for an Enterprise Deployment

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

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

This chapter contains the following topics:

- Section 7.1, "Overview of Preparing Storage for Enterprise Deployment"
- Section 7.2, "Terminology for Directories and Directory Variables"
- Section 7.3, "About File Systems"
- Section 7.4, "About Recommended Locations for the Different Directories"
- Section 7.5, "Configuring Exalogic Storage for Oracle Identity Management"

7.1 Overview of Preparing Storage for Enterprise Deployment

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

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

7.2 Terminology for Directories and Directory Variables

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For more information about, and examples of these variables, see Section 7.4.4, "Recommended Directory Locations."

7.3 About File Systems

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

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

7.4 About Recommended Locations for the Different Directories

This section contains the following topics:

- Section 7.4.1, "Recommendations for Binary (Middleware Home) Directories"
- Section 7.4.2, "Recommendations for Domain Configuration Files"
- Section 7.4.3, "Shared Storage Recommendations for JMS File Stores and Transaction Logs"
- Section 7.4.4, "Recommended Directory Locations"

7.4.1 Recommendations for Binary (Middleware Home) Directories

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

- Section 7.4.1.1, "About the Binary (Middleware Home) Directories"
- Section 7.4.1.2, "About Sharing a Single Middleware Home"
- Section 7.4.1.3, "About Using Redundant Binary (Middleware Home) Directories"

7.4.1.1 About the Binary (Middleware Home) Directories

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

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

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

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

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

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

7.4.1.2 About Sharing a Single Middleware Home

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

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

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

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

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

7.4.1.3 About Using Redundant Binary (Middleware Home) Directories

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

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

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

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

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

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

7.4.1.4 About the Lifecycle Repository

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

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

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

The advantages of having a shared lifecycle repository are:

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

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

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

7.4.2 Recommendations for Domain Configuration Files

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

- Section 7.4.2.1, "About Oracle WebLogic Server Administration and Managed Server Domain Configuration Files"
- Section 7.4.2.2, "Shared Storage Requirements for Administration Server Domain Configuration Files"
- Section 7.4.2.3, "Local Storage Requirements for Managed Server Domain Configuration Files"

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

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

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

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

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

7.4.2.2 Shared Storage Requirements for Administration Server Domain Configuration Files

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

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

7.4.2.3 Local Storage Requirements for Managed Server Domain Configuration Files

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

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

7.4.3 Shared Storage Recommendations for JMS File Stores and Transaction Logs

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

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

7.4.4 Recommended Directory Locations

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

This section includes the following topics:

- Section 7.4.4.1, "Lifecycle Management and Deployment Repository"
- Section 7.4.4.2, "Shared Storage"
- Section 7.4.4.3, "Private Storage"

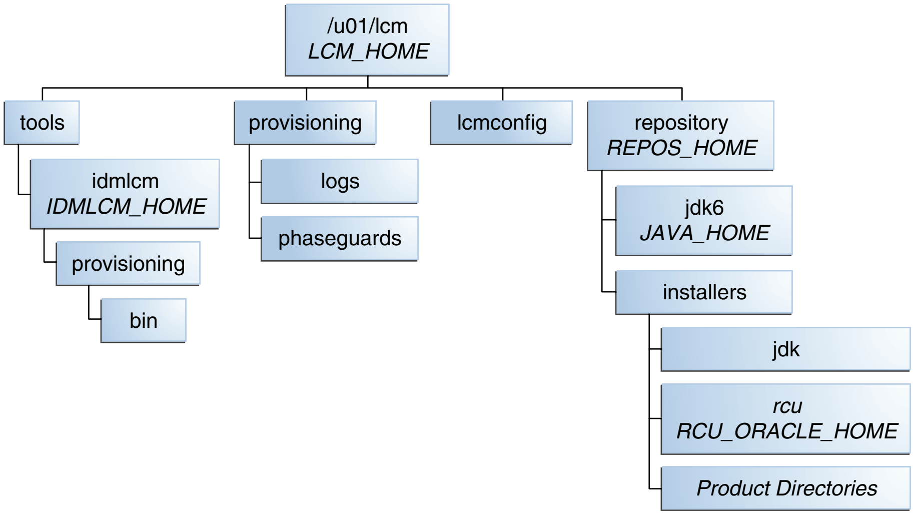
7.4.4.1 Lifecycle Management and Deployment Repository

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

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

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

Figure 7–1 Deployment Repository



7.4.4.2 Shared Storage

I In an enterprise deployment the following shared storage is required. This shared storage must be on shared disk. The mount point must be `/u01/oracle`.

The recommended layout is described in Table 7–1 and Table 7–2 and shown in Figure 7–2.

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

Table 7–1 Volumes on Shared Storage–Distributed Topology

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

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

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

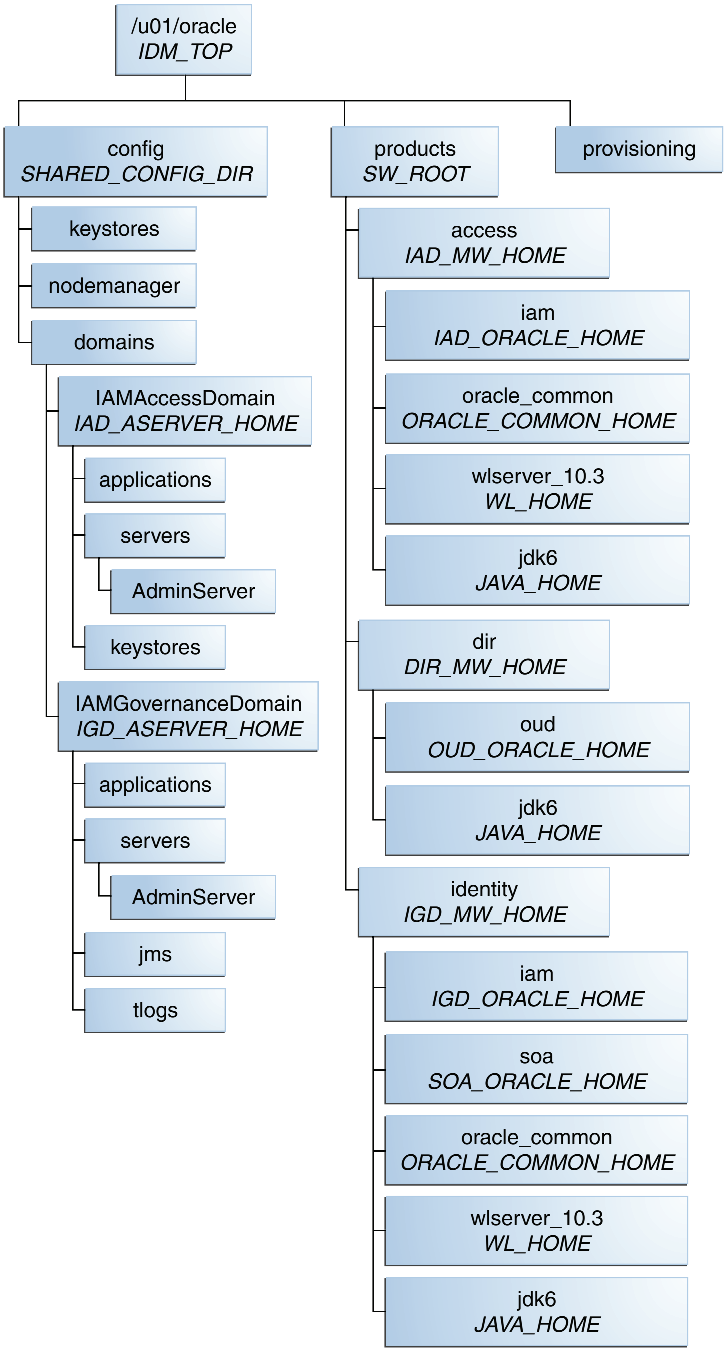
Table 7–2 Volumes on Shared Storage–Consolidated Topology

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

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

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

Figure 7–2 Shared Storage



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

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

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

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

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

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

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

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

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

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

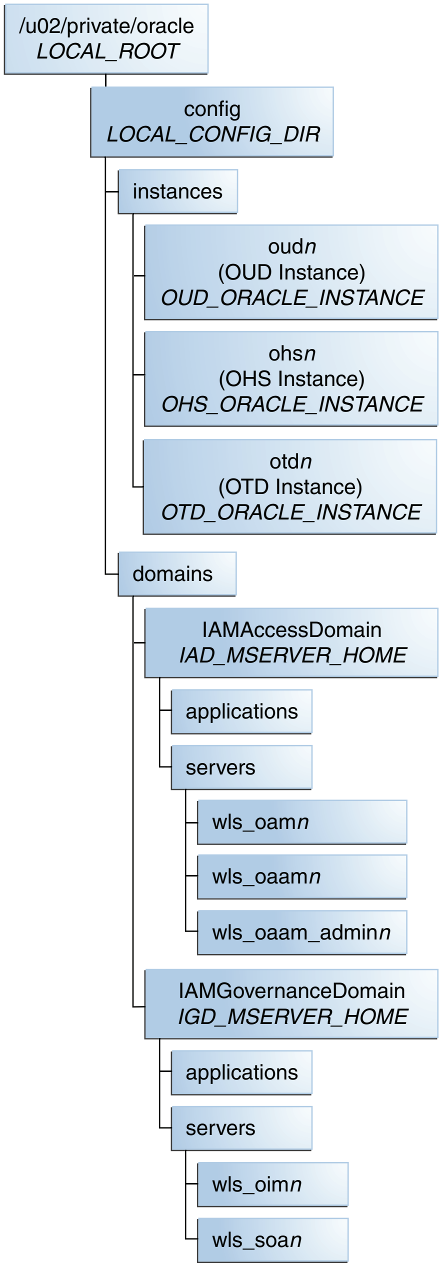
7.4.4.3 Private Storage

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

Table 7–3 Private Storage Directories

Tier	Environment Variable	Directory	Hosts
Web Tier	*WEB_MW_HOME*	/u01/oracle/products/web	WEBHOST1 WEBHOST2
	WEB_ORACLE_INSTANCE	/u02/private/oracle/config/instances/ohs*n*	WEBHOST1 WEBHOST2
	OTD_ORACLE_INSTANCE	/u02/private/oracle/config/instances/otdn	WEBHOST1 WEBHOST2
	OTD_ORACLE_HOME	/u01/oracle/products/web/otd	WEBHOST1/2
	OHS_ORACLE_HOME	/u01/oracle/products/web/ohs	WEBHOST1/2
Application Tier	*OUD_ORACLE_INSTANCE*	/u02/private/oracle/config/instances/oud*n*	LDAPHOST1 LDAPHOST2
	IAD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMAccessDomain	OAMHOST1 OAMHOST2
	IGD_MSERVER_HOME	/u02/private/oracle/config/domains/IAMGovernanceDomain	OIMHOST1 OIMHOST2

Figure 7–3 Private Storage



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

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

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

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

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

Figure 7–4 Private Binary Storage

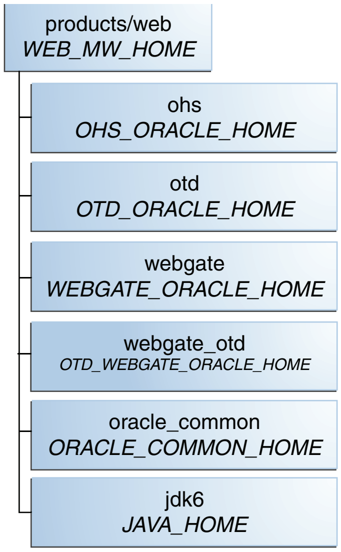


Figure 7–4 shows the local binary storage directory hierarchy. The top level directory, /u01/oracle (), has a subdirectory, products.

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

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

7.5 Configuring Exalogic Storage for Oracle Identity Management

The following sections describe how to configure the Sun ZFS Storage 7320 appliance for an enterprise deployment:

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

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

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

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

Figure 7–6 shows the recommended physical directory structure on the Sun ZFS Storage 7320 appliance.

Table 7–5 shows how the shares on the appliance map to the mount points you will create on the vServers.

Figure 7–5 Physical Structure of the Shares on the Sun ZFS Storage Appliance for Physical Exalogic Deployments

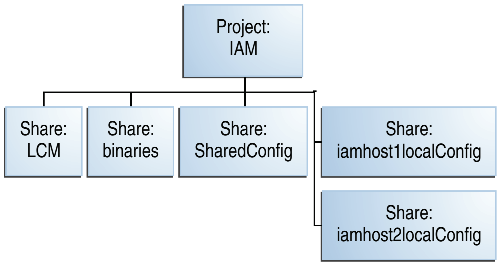


Figure 7–5 illustrates the physical structure of the shares on the Sun ZFS storage appliance

Table 7–4 Mapping the Shares on the Appliance to Mount Points on Each Compute Node

Project	Share	Mount Point	Host	Mounted On	Privileges to Assig to User, Group, an Other
IAM	`binaries`	`/export/IAM/binaries`	IAMHOST1 IAMHOST2	`/u01/oracle/products`	R and W (Read and Write)
IAM	LCM	`/export/IAM/LCM`	ALL Hosts	`/u01/lcm`	R and W (Read and Write)
IAM	`sharedConfig`	`/export/IAM/sharedConfig`	IAMHOST1 IAMHOST2	`/u01/oracle/config`	R and W (Read and Write)
IAM	`iamhost1localConfig`	`/export/IAM/iamhost1localConfig`	IAMHOST1	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`iamhost2localConfig`	`/export/IAM/iamhost2localConfig`	IAMHOST2	`/u02/private/oracle/config`	R and W (Read and Write)

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

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

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

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

Figure 7–6 shows the recommended physical directory structure on the Sun ZFS Storage 7320 appliance.

Table 7–5 shows how the shares on the appliance map to the mount points you create on the vServers that host the enterprise deployment software.

Figure 7–6 Physical Structure of the Shares on the Sun ZFS Storage Appliance for Virtual Exalogic Deployments

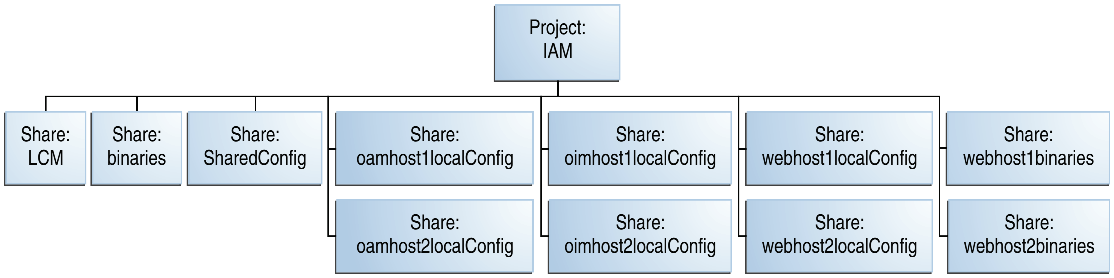

Project: IAM
Share: LCM
Share: binaries
Share: SharedConfig
Share: oamhost1localConfig
Share: oimhost1localConfig
Share: webhost1localConfig
Share: webhost1binaries
Share: oamhost2localConfig
Share: oimhost2localConfig
Share: webhost2localConfig
Share: webhost2binaries

Figure 7–6 illustrates the physical structure of the shares on the Sun ZFS storage appliance.

Table 7–5 Mapping the Shares on the Appliance to Mount Points on Each vServer

Project	Share	Mount Point	Host	Mounted On	Privileges to Assign to User, Group, and Other
IAM	`binaries`	`/export/IAM/binaries`	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	`/u01/oracle/products`	R and W (Read and Write)
IAM	LCM	`/export/IAM/LCM`	ALL Hosts	`/u01/lcm`	R and W (Read and Write)
IAM	`sharedConfig`	`/export/IAM/sharedConfig`	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	`/u01/oracle/config`	R and W (Read and Write)
IAM	`oamhost1localConfig`	`/export/IAM/oamhost1localConfig`	OAMHOST1	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`oamhost2localConfig`	`/export/IAM/oamhost2localConfig`	OAMHOST2	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`oimhost1localConfig`	`/export/IAM/oimhost1localConfig`	OIMHOST1	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`oimhost2localConfig`	`/export/IAM/oimhost2localConfig`	OIMHOST2	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`webhost1localConfig`	`/export/IAM/webhost1localConfig`	WEBHOST1	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`webhost2localConfig`	`/export/IAM/webhost2localConfig`	WEBHOST2	`/u02/private/oracle/config`	R and W (Read and Write)
IAM	`webhost1binaries`	`/export/IAM/webhost1binaries`	WEBHOST1	`/u01/oracle/products`	R and W (Read and Write)
IAM	`webhost2binaries`	`/export/IAM/webhost2binaries`	WEBHOST2	`/u01/oracle/products`	R and W (Read and Write)

Note: The `binary` directories can be changed to **read only** after the configuration is complete if desired.

7.5.3 Preparing Storage for Exalogic Deployment

Prepare storage for the physical Exalogic deployment as described in the following subsections:

- Section 7.5.3.1, "Prerequisite Storage Appliance Configuration Tasks"
- Section 7.5.3.2, "Creating Users and Groups in NIS"
- Section 7.5.3.3, "Creating the IAM Project Using the Storage Appliance Browser User Interface (BUI)"
- Section 7.5.3.4, "Creating the Shares in the IAM Project Using the BUI"

7.5.3.1 Prerequisite Storage Appliance Configuration Tasks

The instructions in this guide assume that the Sun ZFS Storage 7320 appliance is already set up and initially configured. Specifically, it is assumed you have reviewed the following sections in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*:

- "Prerequisites"
- "Getting Started"
- "Sun ZFS Storage 7320 Appliance Overview"
- "Configuration Overview"
- "Naming Service"

7.5.3.2 Creating Users and Groups in NIS

This step is optional. If you want to use the onboard NIS servers, you can create users and groups using the steps in this section.

First, determine the name of your NIS server by logging into the Storage BUI. For example:

1. Log in to the ZFS Storage Appliance using the following URL:

   ```
   https://exalogicsn01-priv:215
   ```

2. Log in to the BUI using the storage administrator's user name (root) and password.
3. Navigate to **Configuration**, and then **Services**.
4. Click on **NIS**

   There is a green dot next to it if it is running. If it is not running and you wish to configure NIS, see the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

5. Click on NIS. you will see the named NIS servers. Make a note of one of the NIS servers.

   Now that you have the name of the NIS server open a terminal window on the NIS server as root and perform the following actions:

6. Create users as described in Section 9.11, "Configuring Users and Groups."
7. Add Users to `yp` by performing the following steps:

a. Navigate to the following directory:

```
/var/yp
```

b. Run the following command:

```
make -C /var/yp
```

c. If required, restart the services using the following commands:

```
service ypserv start
service yppasswdd start
service rpcimapd start
service ypbind start\
```

d. Validate that the users and groups appear in NIS by issuing the command:

```
ypcat passwd
```

and

```
ypcat group
```

7.5.3.3 Creating the IAM Project Using the Storage Appliance Browser User Interface (BUI)

To configure the appliance for the recommended directory structure, you create a custom project, called `IAM`, using the Sun ZFS Storage 7320 appliance Browser User Interface (BUI).

After you set up and configure the Sun ZFS Storage 7320 appliance, the appliance has a set of default projects and shares. For more information, see "Default Storage Configuration" in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

The instructions in this section describe the specific steps for creating a new "IAM" project for the enterprise deployment. For more general information about creating a custom project using the BUI, see "Creating Custom Projects" in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

To create a new custom project called IAM on the Sun ZFS Storage 7320 appliance:

1. Log in to the ZFS Storage Appliance using the URL:

   ```
   https://exalogicsn01-priv:215
   ```

2. Log in to the BUI using the storage administrator's user name (root) and password.
3. Navigate to the **Projects** page by clicking on the **Shares** tab, then the **Projects** sub-tab.

   The BUI displays the Project Panel.
4. Click **Add** next to the **Projects** title to display the Create Project window.

   Enter Name: `IAM`

   Click **Apply**.
5. Click **Edit Entry** next to the newly created **IAM** Project.
6. Click the **General** tab on the project page to set project properties.
7. Update the following values:

- **Mountpoint**: Set to `/export/IAM`
- Under the **Default Settings Filesystems** section:

  User: `oracle`

  Group: `oinstall`

  Permissions: `RWX RWX R_X`

8. For the purposes of the enterprise deployment, you can accept the defaults for the remaining project properties.

   For more information about the properties you can set here, see the "Project Settings" table in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

9. Click **Apply** on the **General** tab to create the IDM project.

7.5.3.4 Creating the Shares in the IAM Project Using the BUI

After you have created the IAM project, the next step is to create the required shares within the project.

The instructions in this section describe the specific steps for creating the shares required for an Oracle Identity Management enterprise deployment. For more general information about creating custom shares using the BUI, see "Creating Custom Shares" in the *Oracle Exalogic Elastic Cloud Machine Owner's Guide*.

Table 7–5 lists the shares required for all the topologies described in this guide. The table also indicates what privileges are required for each share.

Create two additional shares for each of the compute nodes hosting Oracle Traffic Director, as shown in Table 7–5.

To create each share, use the following instructions, replacing the name and privileges, as described in Table 7–5:

1. Login to the storage system BUI, using the following URL:

   ```
   https://ipaddress:215
   ```

   For example:

   ```
   https://exalogicsn01-priv:215
   ```

2. Navigate to the Projects page by clicking the **Shares** tab, and then the **Projects** sub-tab.
3. On the Project Panel, click **IAM**.
4. Click the plus (+) button next to **Filesystems** to add a file system.

   The Create Filesystems screen is displayed.

5. In the Create Filesystems screen, choose **IAM** from the **Project** pull-down menu.
6. In the **Name** field, enter the name for the share.

   Refer to Table 7–5 for the name of each share.

7. From the **Data migration source** pull-down menu, choose **None**.
8. Select the **Permissions** option and set the permissions for each share.

   Refer to Table 7–5 for the permissions to assign each share.

9. Select the **Inherit Mountpoint** option.

10. To enforce UTF-8 encoding for all files and directories in the file system, select the **Reject non UTF-8** option.
11. From the **Case sensitivity** pull-down menu, select **Mixed**.
12. From the **Normalization** pull-down menu, select **None**.
13. Click **Apply** to create the share.

Repeat the procedure for each share listed in Table 7–5.

7.5.3.5 Allowing Local Root Access to Shares

If you want to run commands or traverse directories on the share as the root user, you must add an NFS exception to allow you to do so. You can create exceptions either at the individual, share, or project level.

To keep things simple, in this example you create the exception at the project level.

To create an exception for NFS at the project level:

1. In the Browser User Interface (BUI), access the Projects user interface by clicking **Configuration**, **STORAGE**, **Shares**, and then **Projects**.

   The Project Panel appears.
2. On the Project Panel, click **Edit** next to the project **IAM**.
3. Select the **Protocols** tab.
4. Click the **+** sign next to NFS exceptions.
5. Select **Type: network**.
6. In the **Entity** field, enter the IP address of the compute node as it appears on the Storage Network (bond0) in CIDR format. For example: 192.168.10.3/19

   ```
   192.168.10.3/19
   ```
7. Set **Access Mode** to **Read/Write** and check **Root Access**.
8. Click **Apply**.
9. Repeat for each compute node that accesses the ZFS appliance.

8 Creating Exalogic Virtual Servers (vServers)

This chapter describes how to create Exalogic Virtual Servers (vServers).

It contains the following sections:

8.1 Prerequisites

Before starting an Exalogic Deployment ensure that the following tasks have been performed:

1. Exalogic rack has been commissioned and one-command run.
2. Accounts have been created in Exalogic Control.
3. Private IPoIB network has been created for the account, enabling secure communications between the Virtual Servers assigned to the Account as described in Section 6.4.2, "Creating a Private IPoIB Network,"
4. You have created and loaded a Server Template for the operating system you wish to deploy.
5. You have created a vServer Type which matches the specification of the Virtual Servers you want to create.
6. A Client Access Network has been created, using a bonded Network Interface for communication between the vServers and an External Load Balancer.

8.2 Distribution Groups

A Distribution group prevents virtual servers assigned to it from running on the same physical nodes. By preventing different vServers of the same type running on the same physical server, you prevent the failure of the underlying physical server from taking out the complete system.

In an IAM Exalogic implementation, three Distribution Groups are required:

- IAM_OTD: Prevents two Oracle Traffic Director Servers from running on the same Physical Server
- IAM_IAD: Prevents two IAMAccessDomain Servers from running on the same Physical Server
- IAM_IAG: Prevents two IAMGovernanceDomain Servers from running on the same physical server

8.2.1 Creating a Distribution Group

To Create a distribution group perform the following steps:

1. Log in to Exalogic Control at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Expand **vDC Management**.
3. Navigate to **vDCs - Accounts - Cloud Admin Account**.
4. In the actions window click **Create Distribution Group**.
5. Enter a **Name**, for example: `IAM_OTD`.
6. Click **Next**.
7. Enter **Number of Elements**.

   This is a number that defines the number of Oracle VM Servers on which the vServers can be placed. For example, where OTD can run on two vServers, then the number of elements is 2.
8. Click **Next**.
9. Click **Finish**.

Repeat for each Distribution Group to be created. Table 8–1 lists Distribution Groups and the number of elements for each.

Table 8–1 Number of Elements for Distribution Groups

Distribution Group	Number of Elements
IAM_OTD	2
IAM_IAD	2
IAM_IAG	2

8.3 Create Virtual Servers (vServer)

The vServerTypes are based on the supplied Exalogic vServerTypes. Depending on your load you may need to increase the size of the default template requirements.

Table 8–2 vServer Information

Name	vServerType	Virtual Networks	Host Name	Distribution Group
webhost1	LARGE	IPoIB-IAM[1] EoIB-client[2] IPoIB-vserver-shared-storage[3]	webhost1 webhost1-ext webhost1-stor	IAM_OTD
webhost2	LARGE	IPoIB-IAM EoIB-client IPoIB-vserver-shared-storage	webhost2 webhost2-ext webhost2-stor	IAM_OTD
oamhost1	EXTRA_LARGE	IPoIB-IAM EoIB-client IPoIB-vserver-shared-storage	oamhost1 oamhost1-ext oamhost1-stor	IAM_IAD
oamhost2	EXTRA_LARGE	IPoIB-IAM EoIB-client IPoIB-vserver-shared-storage	oamhost2 oamhost2-ext oamhost2-stor	IAM_IAD
oimhost1	EXTRA_LARGE	IPoIB-IAM EoIB-client IPoIB-vserver-shared-storage	oimhost1 oimhost1-ext oimhost1-stor	IAM_IAG
oimhost2	EXTRA_LARGE	IPoIB-IAM EoIB-client IPoIB-vserver-shared-storage	oimhost2 oimhost2-ext oimhost2-stor	IAM_IAG

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

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

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

If your database is on an Exadata machine, you must also include the virtual Network IPoIB-default.

> **Note:** If are planning to use OAAM in your topology, add extra memory to the virtual servers hosting OAM. The extra memory should be at least an additional 4GB.

8.4 Creating vServer Volumes

When you create a vServer, by default, it creates one default volume and allocates the space to swap and the root file system. For a more efficient controlled way to do this, create separate volumes for each vServer to mount for the swap and temp space.

To create separate volumes for each vServer:

1. Log in to Exalogic Control at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Expand **vDC Management**.
3. Navigate to **vDCs**, **Accounts**, and then **Cloud Admin Account**.
4. Select **Create Volume** from the **Actions** menu.
5. Give the volume a name, for example **vServer1_tmp**, and a description.
6. Click **Next**.
7. On the **Volume Configuration** screen, enter a size for the volume.

Do not select **shared**.

8. Click **Next**.
9. On the **Volume Summary** screen, click **Finish** to create the volume.
10. Repeat for each volume to be created.

8.5 About vServer Types

Table 8–3 lists the vServer types used in this document. These vServer types can be used as a guide. Refer to the *Oracle® Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* for the latest hardware requirements.

Table 8–3 vServer Types

vServer Type	Memory	Swap Space	Tmp Space
LARGE	8GB	16GB	2GB
EXTRA_LARGE	16GB	16GB	2GB

8.6 Creating a vServer

To Create a vServer perform the following steps. Refer to Table 8–2, " vServer Information" for data values.

1. Log in to Exalogic Control at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Expand **vDC Management**.
3. Navigate to **vDCs - Accounts - Cloud Admin Account**.
4. In the **Actions** window, click **Create vServer**.
5. Enter:
   - **Name**: For example: `otdhost1`
   - **Number of vServers**:`1`

   Select: **Support High Availability**
6. Click **Next**.
7. Choose the Server Template you want to deploy.
8. Click **Next**.
9. Choose the vServer Type you wish to create, for example: **LARGE**
10. If you have created volumes for `swap` and `tmp`, select them here.
11. Click **Next**.
12. Enter all of the virtual networks you want to assign
13. For each chosen network enter the following:
    - **IP Address Type** - Static or Automatic
    - **IP Address** - Enter the IP address if you have a predetermined IP address to use.

- **Hostname** - Select the fully qualified host name you wish to assign to the IP address.

14. Click **Next**.
15. Enter the Distribution Group to use.
16. Click **Next**.
17. Click **Next** on vServerAccessControl screen.
18. Click **Finish**.

Repeat for Each vServer to be created.

> **Note:** Make sure that each vServer has the swap space detailed in Section 9.4, "Meeting Operating System Requirements."

8.7 Updating vServers

Now that the vServers have been created you need to perform the steps in the following sections to make them available for use.

- Section 8.7.1, "Update the root password"
- Section 8.7.2, "Update hosts File"
- Section 8.7.3, "Post Network Configuration"
- Section 8.7.4, "Set MTU size on InfiniBand Interfaces"

8.7.1 Update the root password

When the vServer is created, it has a default password which is generally `ovsroot`. Change this to a value appropriate to your organization.

8.7.2 Update hosts File

After configuration, your `hosts` file will look something like:

```
IP Address   Host_Name
```

For example:

```
192.168.32.3 oamhost1-stor
```

Change the `hosts` file so that it contains both fully qualified and short names for each network, for example:

```
192.168.10.3 oamhost1.mycompany.com oamhost1
192.168.32.3 oamhost1-stor.mycompany.com oamhost1-stor
192.168.10.3 oamhost1-data.mycompany.com oamhost1-data
```

> **Notes:**
>
> - For clarity the host name of the default network has been changed to `-data` to show it is the network that is used for Exadata communication.
> - External Network interface names are assumed to be in DNS.

8.7.3 Post Network Configuration

Now that your vServer has been created you must configure it as appropriate to your organization.   This typically includes the following steps:

- Section 8.7.3.1, "Determine vServer Storage IP Address"
- Section 8.7.3.2, "Determine Storage Appliance IP Address"

8.7.3.1 Determine vServer Storage IP Address

When you created your vServer, you added the network IPoIB-vserver-shared-storage. This is the network the vServers use to communicate with the ZFS storage appliance. In order for them to communicate properly, you must determine the appropriate IP address of the storage appliance to use.

To determine the IP address perform the following steps:

1. Log in to Exalogic Control as a Cloud User.
2. From the navigation pane on the left, select **vDC Management**.
3. Under vDC Accounts, expand the name of your account, and select the vServer for which you want to configure access to the storage appliance.

   The vServer dashboard is displayed.
4. Select the **Network** tab, and note the IP address of the vServer for the IPoIB-vserver-shared-storage network. This corresponds with the `-stor` entry in the `/etc/hosts` file

   For example: `172.17.0.100`

8.7.3.2 Determine Storage Appliance IP Address

1. Log in to the storage appliance as root. For example, type:

   ```
   ssh root@exalogicsn01.mycompany.com
   ```

2. Show the network interfaces using the command:

   ```
   configuration net interfaces show
   ```

3. The output is similar to the following:

   ```
   configuration net interfaces show
   Interfaces:

   INTERFACE   STATE    CLASS LINKS       ADDRS                   LABEL
   igb0        up       ip    igb0        10.244.64.60/21         igb0
   igb1        offline  ip    igb1        10.244.64.61/21         igb1
   ipmp1       up       ipmp  pffff_ibp1  192.168.10.15/24        ipmp1
                              pffff_ibp0
   ipmp2       up       ipmp  p8001_ibp0  192.168.20.9/24         IB_IF_8001
                              p8001_ibp1
   ipmp3       up       ipmp  p8002_ibp0  192.168.21.9/24         IB_IF_8002
                              p8002_ibp1
   ipmp4       up       ipmp  p8005_ibp0  172.17.0.9/16           IB_IF_8005
                              p8005_ibp1
   p8001_ibp0  up       ip    p8001_ibp0  0.0.0.0/8               ibp0.8001
   p8001_ibp1  up       ip    p8001_ibp1  0.0.0.0/8               ibp1.8001
   p8002_ibp0  up       ip    p8002_ibp0  0.0.0.0/8               ibp0.8002
   p8002_ibp1  up       ip    p8002_ibp1  0.0.0.0/8               ibp1.8002
   p8005_ibp0  up       ip    p8005_ibp0  0.0.0.0/8               ibp0.8005
   p8005_ibp1  up       ip    p8005_ibp1  0.0.0.0/8               ibp1.8005
   ```

```
pffff_ibp0  up       ip    pffff_ibp0  0.0.0.0/8              ibp0
pffff_ibp1  up       ip    pffff_ibp1  0.0.0.0/8              ibp1
```

4. Determine the corresponding IP address by looking for the IP address in the same range as 172.17.0.100. In this example it is the one associated with interface ipmp4, for example: 172.17.0.9.

5. Create an entry in the `/etc/hosts` file to reflect this, for example:

```
172.17.0.9  zfsinternal.mycompany.com  zfsinternal
```

8.7.4 Set MTU size on InfiniBand Interfaces

In order to maintain optimum performance, you must update the MTU size of each of the InfiniBand interfaces on the vServer to 65520. To do this perform the following steps:

1. Log in to the vServer as the `root` user.

2. Verify the current MTU for `bond2` by running the `ifconfig` command.

> **Note:** The steps in this procedure use `bond2` as an example. This procedure should be repeated for all the InfiniBand interfaces.

```
ifconfig bond2
bond2     Link encap:InfiniBand  HWaddr
          80:58:08:CA:FE:80:00:00:00:00:00:00:00:00:00:00:00:00:00:00
          inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:504 (504.0 b)  TX bytes:420 (420.0 b)
```

3. Append the line `MTU=64000` to the `ifcfg` file corresponding to the `bond2` interface:

```
echo MTU=64000 >> /etc/sysconfig/network-scripts/ifcfg-bond2
```

4. Verify whether the `MTU=64000` line was added to the `ifcfg-bond2` file:

```
cat /etc/sysconfig/network-scripts/ifcfg-bond2 | grep MTU
MTU=64000
```

5. Find the slave interfaces for `bond2`:

```
cd /etc/sysconfig/network-scripts
grep "MASTER=bond2" ifcfg-* | awk -F":" '{print $1}'
ifcfg-ib0.8009
ifcfg-ib1.8009
```

6. Set the mode to `connected` for both the slave interfaces of the `bond2` interface:

```
echo connected > /sys/class/net/ib0.8009/mode
echo connected > /sys/class/net/ib1.8009/mode
```

7. Perform Steps 2 through 6 for the other InfiniBand interfaces.

8. Stop and start the vServer as described in Section 20.1.4, "Stopping and Starting vServers."

9. After the vServer starts, log in again to the vServer using SSH as the root user.
10. Run the ifconfig command for each InfiniBand interface, and verify that the output of the command displays MTU:64000, as shown in the following example for bond2 and its slave interfaces:

    ```
    ifconfig bond2 | grep MTU
    UP BROADCAST RUNNING MASTER MULTICAST  MTU:64000  Metric:1

    ifconfig ib0.8009 | grep MTU
    UP BROADCAST RUNNING SLAVE MULTICAST  MTU:64000  Metric:1

    ifconfig ib1.8009 | grep MTU
    UP BROADCAST RUNNING SLAVE MULTICAST  MTU:64000  Metric:1
    ```

8.8 Move Swap and TMP to Separate Volumes

If you create separate disk volumes for swap and tmp, update your vServer to use these new volumes.

The disk volumes are added to your virtual server as virtual volumes. They appear in the /dev directory as xvdb/c.

To determine the exact names, run the following command:

```
fdisk -l
```

This command shows output similar to:

```
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c520c

Device Boot Start End Blocks Id System
/dev/xvda1 * 1 32 256000 83 Linux
Partition 1 does not end on cylinder boundary.
/dev/xvda2 32 1305 10223616 8e Linux LVM

Disk /dev/xvdb: 18.3 GB, 18253611008 bytes
255 heads, 63 sectors/track, 2219 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/xvdc: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

As you can see from the output, /dev/xvda has a partition created on it so it is in use. This is the default disk.

Disks /dev/xvdb and /dev/xvdc do not have a partition and are therefore the attached disk volumes. You can determine which is which by the size of the volumes.

To use these volumes in the vServer, create a partition of type LVM. This enables the use of Linux LVM, and make resizing easier if required later. The procedure is the same if you are using the disk for `swap` or `tmp`.

To create an LVM partition:

1. Choose a disk to work on using the following command:

   ```
   fdisk disk_name
   ```

   For example:

   ```
   fdisk /dev/xvdb
   ```

2. When prompted for a command type `n`
3. You are asked if you wish to create an extended or primary partition. Select `p` for primary.
4. When promoted for a partition number, enter `1`.
5. You are then asked where on the disk to create the partition. Accept the Default from value of `1`. Accept the default end value to use the entire disk.
6. Now that the partition has been created, give it a type. To do this, when prompted for a command, enter `t`.
7. You can see the list of types available by entering the command `L`.
8. When prompted for the Hex code, enter the code (from the previous list) for the Linux LVM. This is typically `8e`.
9. Save your changes using the command `w`.
10. Validate that the changes are correct using the command `fdisk -l`
11. Repeat the procedure for each disk volume

Now that you have disk partitions, create logical volumes to use those disks:

1. Create a physical volume on the disk partition by using the command:

   ```
   pvcreate disk_partition
   ```

   For example

   ```
   pvcreate /dev/xvdb1
   ```

   > **Note:** The number `1` at the end of the disk, which denotes the partition number, is the same as the values you saw in the `fdisk -l` command.

   Repeat for each disk partition you created above.

2. Verify that the physical volumes have been created correctly using the following command

   ```
   pvdisplay
   ```

3. Create a volume group, one for each virtual disk. You can create a single volume group for all disks, but this example uses one per disk.

   To create a volume group, use the following command:

```
vgcreate volume_group_name disk partition
```

For example:

```
vgcreate volGroupSwap /dev/xvdb1
```

Repeat for each volume group. For example: `volGroupTemp` `volGroupSwap`.

4. Validate that the volume groups have been created properly using the following:

   ```
   vgdisplay
   ```

5. Once you've created the volume groups, create a logical volume inside the volume group using the following command:

   ```
   lvcreate --name lvname --size 40G volume_group
   ```

   `size` is the size of space you wish to assign to the volume group. This equates to the size of the file system.

   For example

   ```
   lvcreate ---name Swap1 ---size 16G volGroupSwap
   ```

   Repeat for each logical volume to be created.

6. Validate that the logical volumes were created successful using the following command:

   ```
   lvdisplay
   ```

Creating a Swap File on the New Logical Volume

To use a logical volume for `swap`:

1. Create a swapfile using the following command

   ```
   mkswap volume_group
   ```

   For example:

   ```
   mkswap /dev/volGroupSwap/Swap1
   ```

2. Create an entry in the `/etc/fstab` directory for the new `swap` file. The entry will look similar to:

   ```
   /dev/volGroupSwap/Swap1 swap swap defaults 0 0
   ```

   Comment out the original swap entry.

3. Validate that the new swap space is being used by issuing the command swapon -s

   You can disable the original swap using the following command:

   ```
   swapoff
   ```

> **Note:** This is not necessary as only your new swap space will be available after a reboot.

Moving /tmp to the New Logical Volume

If you have created a logical volume for `/tmp`, you can enable this by first creating a file system on it and then mounting it as a disk. You do this by performing the following commands:

1. Create a file system using the command:

   ```
   mkfs.ext3 volume_name
   ```

   For example:

   ```
   mkfs.ext3 /dev/volGroupTemp/Temp1
   ```

2. Add the new file system to `/etc/fstab` so that it is automatically mounted.

   Create an entry similar to:

   ```
   /dev/volGroupTemp/Temp1 /tmp ext3 defaults 1 1
   ```

3. Mount the file system using the following command

   ```
   mount -a
   ```

4. Verify that the file system is created correctly using the following command:

   ```
   df -k
   ```

9 Configuring the Servers for an Enterprise Deployment

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

It contains the following sections:

9.1 Overview of Configuring the Servers

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

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

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

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

9.2 Verifying Your Server and Operating System

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

9.3 Meeting the Minimum Hardware Requirements

In order to use a server in an Oracle Enterprise Deployment you must verify that it meets the minimum specification described in Section 3.6, "Hardware Requirements for the Identity Management on Exalogic." If you plan to use a different deployment architecture, for example, one with more or fewer components deployed on a different number of boxes, you must check *Oracle® Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* to ensure that you have the minimum specification to support the products you plan to deploy on these servers.

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

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

Allow sufficient swap and temporary space. Specifically:

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

9.4 Meeting Operating System Requirements

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

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

This section includes the following topics:

- Section 9.4.1, "Configure Kernel Parameters."
- Section 9.4.2, "Setting the Open File Limit."
- Section 9.4.3, "Setting Shell Limits."
- Section 9.4.4, "Configuring Local Hosts File."
- Section 9.4.5, "Increase Huge Page Allocation."

9.4.1 Configure Kernel Parameters

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

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

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

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

Table 9–1 UNIX Kernel Parameters

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

To set these parameters:

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

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

9.4.2 Setting the Open File Limit

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

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

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

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

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

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

9.4.3 Setting Shell Limits

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

Most Linux Versions

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

Add the following lines:

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

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

Oracle Linux 6 and Red Hat Enterprise Linux 6 Only

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

Add the following lines:

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

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

Add the following lines:

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

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

After editing the file, reboot the machine.

9.4.4 Configuring Local Hosts File

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

`IP_Address Fully_Qualified_Name Short_Name`

For example

```
192.168.30.1 oimhost1vhn.mycompany.com oimhost1vhn

192.168.30.2 oimhost2vhn.mycompany.com oimhost2vhn

192.168.30.3 soahost1vhn.mycompany.com soahost1vhn

192.168.30.4 soahost2vhn.mycompany.com soahost2vhn

192.168.50.1 idstore.mycompany.com idstore

192.168.50.2 idminternal.mycompany.com idminternal

192.168.10.1 iamhost1.mycompany.com iamhost1

192.168.10.2 iamhost2.mycompany.com iamhost2

192.168.10.1 webhost1.mycompany.com webhost1

192.168.10.2 webhost2.mycompany.com webhost2
```

Note:

- If `idstore.mycompany.com` and `idminternal.mycompany.com` have DNS entries, you do not need to add to the `/etc/hosts`.
- If using virtual Exalogic, entries for IAMHOSTs should be replaced with entries for OAMHOSTs and OIMHOSTs

9.4.5 Increase Huge Page Allocation

By default huge pages are enabled in Exalogic compute nodes, verify the existing allocation by running.

```
grep Huge /proc/meminfo
```

Set the recommended Huge Page allocation to `25000`.

To set the Huge Page allocation, run the following command as root in the compute node:

```
echo 25000  > /proc/sys/vm/nr_hugepages
```

9.5 Enabling Unicode Support

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

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

Set the LANGUAGE environment variable as follows:

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

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

9.6 Set DNS Setting

Configure the vServer to access your corporate DNS Servers. To do this, update DNS settings by updating the file `/etc/resolv.conf`.

9.7 Configuring a Server to Use an NIS/YP Server

If you are using NFS Version 4, configure a directory service or an NIS (Network Information Server). If your organization does not have one already, use the built-in one on the ZFS storage appliance. See Configuring NFS Version 4 (NFSv4) on Exalogic in the *Oracle Fusion Middleware Exalogic Machine Owner's Guide* for more information.

Once you have configured your NIS server, configure each compute node to use it. If you are using the built-in NIS server on the Exalogic ZFS appliance, use the following steps:

1. Determine the name of the NIS server by logging into the storage BUI using the URL:

   ```
   https://exalogicsn01-priv:215
   ```

2. Click **Configuration**, **Services**, and then **NIS**.
3. Make a note of one of the listed NIS servers.
4. Login to the compute node as root.

5. Edit the `/etc/idmapd.conf` configuration file:

   ```
   vi /etc/idmapd.conf
   ```

   Set the domain value, as in the following example:

   ```
   Domain = mycompany.com
   ```

6. Restart the `rpcidmapd` service:

   ```
   service rpcidmapd restart
   NISDOMAIN=mycompany.com
   ```

7. Update the `/etc/yp.conf` configuration file, and set the correct domain value, as in the following example:

   ```
   vi /etc/yp.conf
   ```

   Add the following line:

   ```
   domain mycompany.com server NIS_Server_hostname_or_IP
   ```

   Where `mycompany.com` is the example domain and *NIS_Server_hostname_or_IP* is the host name or IP address of the NIS server. You must replace these sample values with values appropriate for your environment.

8. Set NIS domain name on the command line:

   ```
   domainname NIS_DOMAIN_NAME
   ```

   For example:

   ```
   domainname nisdomain.example.com
   ```

9. Edit the `/etc/nsswitch.conf` configuration file:

   ```
   vi /etc/nsswitch.conf
   ```

   Change the following entries:

   ```
    passwd:     files nis
    shadow:     files nis
    group:      files nis
    automount:  files nis nisplus
    aliases:    files nis nisplus
   ```

10. Restart the `rpcidmapd` service:

    ```
    service rpcidmapd restart
    ```

11. Edit the file `/etc/sysconfig/network` and add the following line:

    ```
    NISDOMAIN=mycompany.com
    ```

12. Restart the `ypbind` service by running the following command:

    ```
    service ypbind restart
    ```

13. Check the `yp` service by running this command:

    ```
    ypwhich
    ```

14. Verify if you can access Oracle user accounts:

    ```
    ypcat passwd
    ```

15. Add ypbind to your boot sequence, so that it starts automatically after rebooting.

    ```
    chkconfig ypbind on
    ```

9.8 Enabling Virtual IP Addresses

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

Chapter 4, "Networking Overview" describes the mapping of IP Addresses to servers.

This section includes the following topics:

- Section 9.8.1, "Summary of Exalogic Physical Virtual IP Addresses"
- Section 9.8.2, "Summary of Exalogic Logical Virtual IP Addresses"
- Section 9.8.3, "Enabling a Virtual IP Address on a Network Interface"
- Section 9.8.4, "Verifying the Required Virtual IP Addresses on the Network"

9.8.1 Summary of Exalogic Physical Virtual IP Addresses

For all communications over the IPoIB network, the IAMHOST compute nodes and WebLogic Server managed servers use the default bond0 IP addresses assigned when the Exalogic hardware was commissioned.

Table 9–3 lists the Virtual IPs you must define for the Access Manager and Oracle Identity Manager Managed Servers on IAMHOST1 and IAMHOST2.

For instructions on defining these virtual IP addresses, see Section 9.8.3, "Enabling a Virtual IP Address on a Network Interface."

Table 9–2 Physical Virtual IP Addresses Associated with IPoIB and EoIB Network interfaces

Interface	Address Example	Netmask Example	Used By	Virtual Host Name	Default Physic Host[1]
BOND1:1	10.10.30.1	255.255.224.0	OTD Administration Server		IAMHOST1
BOND1:1	10.10.30.2	255.255.224.0	Administration Server (IADADMINVHN)		IAMHOST1
BOND1:2	10.10.30.3	255.255.224.0	Administration Server (IGDADMINVHN)		IAMHOST1
BOND0:1	192.168.30.1	255.255.240.0	WLS_OIM1	OIMHOST1VHN	IAMHOST1
BOND0:1	192.168.30.2	255.255.240.0	WLS_OIM2	OIMHOST2VHN	IAMHOST2
BOND0:2	192.168.30.3	255.255.240.0	WLS_SOA1	SOAHOST1VHN	IAMHOST1
BOND0:2	192.168.30.4	255.255.240.0	WLS_SOA2	SOAHOST2VHN	IAMHOST2
BOND0:1	192.168.50.1	255.255.224.0	OTD Failover group for SOA	IDMINTERNAL	IAMHOST1
BOND0:1	192.168.50.2	255.255.224.0	OTD Failover group for OUD	IDSTORE	IAMHOST2

[1] Default Physical Host is the compute Node used in a physical exalogic deployment

Note: Physical IP addresses are managed manually. Oracle Traffic Director IP Addresses are handled by Oracle Traffic Director.

9.8.2 Summary of Exalogic Logical Virtual IP Addresses

For all communications over the IPoIB network, the WEBHOST compute nodes and WebLogic Server managed servers use the default `bond0` IP addresses assigned when the Exalogic hardware was commissioned.

Table 9–3 lists the Virtual IPs you must define for the Access Manager and Oracle Identity Manager Managed Servers on IAMHOST1 and IAMHOST2.

For instructions on defining these virtual IP addresses, see Section 9.8.3, "Enabling a Virtual IP Address on a Network Interface."

Table 9–3 Logical Virtual IP Addresses Associated with IPoIB Network interfaces

Interface	Address Example	Netmask Example	Used By	Virtual Host Name	Default Virtual Host[1]
BOND1:1	10.10.30.1	255.255.224.0	OTD Administration Server		WEBHOST1
BOND1:2	10.10.30.2	255.255.224.0	Administration Server (IADADMINVHN)		OAMHOST1
BOND1:3	10.10.30.3	255.255.224.0	Administration Server (IGDADMINVHN)		OIMHOST1
BOND0:1	192.168.30.1	255.255.240.0	WLS_OIM1	OIMHOST1VHN	OIMHOST1
BOND0:1	192.168.30.2	255.255.240.0	WLS_OIM2	OIMHOST2VHN	OIMHOST2
BOND0:2	192.168.30.3	255.255.240.0	WLS_SOA1	SOAHOST1VHN	OIMHOST1
BOND0:2	192.168.30.4	255.255.240.0	WLS_SOA2	SOAHOST2VHN	OIMHOST2

[1] Default Virtual Host is the vServer used in the Virtual Exalogic Deployment.

Note: The virtual IP addresses used here are examples. You should use the IP addresses you reserved in Part 6.4.3, "Reserving Virtual IP Addresses."

9.8.3 Enabling a Virtual IP Address on a Network Interface

To enable the virtual IP addresses listed in Table 9–2 and Table 9–3 on IAMHOST1 and IAMHOST2:

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

```
ifconfig subinterface virtual_ip_address netmask netmask_value
```

   For example, on IAMHOST1, enter the following:

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

Note: the example in this section is applicable for both physical and virtual Exalogic deployments.

---

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

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

9.8.4 Verifying the Required Virtual IP Addresses on the Network

Check that each node can communicate with each other node using both physical and virtual host names for example:

```
ping -I bond0 WEBHOST1 (192.168.10.1)
ping -I bond0 WEBHOST2 (192.168.10.2)
ping -I bond0 IAMHOST1 (192.168.10.3)
ping -I bond0 IAMHOST2 (192.168.10.4)
ping -I bond0 OIMHOST1VHN (192.168.30.1)
ping -I bond0 OIMHOST2VHN (192.168.30.2)
ping -I bond0 SOAHOST1VHN (192.168.30.3)
ping -I bond0 SOAHOST2VHN (192.168.30.4)
```

9.9 Disable Automatic Path Migration from SDP

This step is only required if you have an Exadata Machine connected to the Exalogic machine and you want to connect to the database using SDP.

This addresses an issue where Automatic Path migration can cause the database to stop responding.

1. Add `'sdp_apm_enable=0'` and `'ib_sdp'` option in `/etc/modprobe.conf` file. For example, once it is added, it should output as follows:

   ```
   cat /etc/modprobe.conf | grep ib_sdp
   alias net-pf-27 ib_sdp
   options ib_sdp sdp_zcopy_thresh=0 recv_poll=0 sdp_apm_enable=0
   ```

   Save the file.

2. Reload the ib_sdp driver as follows:

   ```
   modprobe -r ib_sdp
   modprobe ib_sdp
   ```

3. Validate that the change took effect by executing the command:

   ```
   cat /sys/module/ib_sdp/parameters/sdp_apm_enable
   ```

   The result should be 0

9.10 Mounting Shared Storage onto the Host

As shown in Chapter 7, "Preparing Storage for an Enterprise Deployment," you must make shared storage available to each host that will use it.

9.10.1 Shared Storage Overview

Mount the shared storage to the hosts according to one of the following tables, depending on whether you are using physical or virtual Exalogic.

Table 9–4 Mapping the Shares on the Appliance to Mount Points on Each Compute Node

Volume Mounted	Mounted on Host	Mounted Point	Exclusive
/export/IAM/binaries	IAMHOST1 IAMHOST2	/u01/oracle/products	No
/export/IAM/LCM	ALL Hosts	/u01/lcm	No
/export/IAM/sharedConfig	IAMHOST1 IAMHOST2	/u01/oracle/config	No
/export/IAM/iamhostlocalConfig	IAMHOST1	/u02/private/oracle/config	Yes
/export/IAM/iamhost2localConfig	IAMHOST2	/u02/private/oracle/config	Yes

Table 9–5 Mapping the Shares on the Appliance to Mount Points on Each vServer

Volume Mounted	Mounted on Host	Mounted Point	Exclusive
/export/IAM/binaries	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	/u01/oracle/products	No
/export/IAM/LCM	All Hosts	/u01/lcm	No
/export/IAM/sharedConfig	OAMHOST1 OAMHOST2 OIMHOST1 OIMHOST2	/u01/oracle/config	No
/export/IAM/oimhost1localconfig	OIMHOST1	/u02/private/oracle/config	Yes
/export/IAM/oimhost2localconfig	OIMHOST2	/u02/private/oracle/config	Yes
/export/IAM/oamhost1localConfig	OAMHOST1	/u02/private/oracle/config	Yes
/export/IAM/oamhost2localConfig	OAMHOST2	/u02/private/oracle/config	Yes
/export/IAM/webhost1localConfig	WEBHOST1	/u02/private/oracle/config	Yes
/export/IAM/webhost2localConfig	WEBHOST2	/u02/private/oracle/config	Yes
/export/IAM/webhost1binaries	WEBHOST1	/u02/prívate/oracle/products	Yes
/export/IAM/webhost2binaries	WEBHOST2	/u02/prívate/oracle/products	Yes

Note the following points:

- Each host must have appropriate privileges set within the NAS or SAN so that it can write to the shared storage.
- Temporary mounts are only required during provisioning and patching.
- If your directory tier is placed into a dedicated zone, you must share the ORACLE_BASE between the two directory hosts in a distributed topology.
- If WEBHOST1 and WEBHOST2 are in the DMZ, ORACLE_BASE is not shared between those two hosts.

  The mount point should be owned by the user and group created in Section 9.11, "Configuring Users and Groups."

- Follow the best practices of your organization for mounting shared storage. This section provides an example of how to do this on UNIX or Linux using NFS storage.

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

9.10.2 Mounting Shared Storage

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

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

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

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

For example:

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

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

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

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

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

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

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

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

9.10.3 Validating the Shared Storage Configuration

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

For example:

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

Verify that the owner and permissions are correct:

```
ls -l testfile
```

Then remove the file:

```
rm testfile
```

9.11 Configuring Users and Groups

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

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

Groups

You must create the following groups on each node.

- oinstall
- dba

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

```
groupadd groupname
```

For example

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

Users

You must create the following users on each node.

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

Notes:

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

To create users use the following command as root:

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

For example:

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

10

Preparing the Database for an Enterprise Deployment

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

This chapter contains the following topics:

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

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

- Verify the database requirements as described in Section 10.2, "Verifying the Database Requirements for an Enterprise Deployment."
- Install and configure the Oracle database repositories. See the installation guides listed in the "Related Documents" section of the Preface and Section 10.3, "Installing the Database for an Enterprise Deployment."
- Create database services, as described in Section 10.4, "Creating Database Services."
- Prepare the database for the Repository Creation Utility (RCU). See Section 11.2, "Creating an Oracle Identity and Access Management Software Repository."
- Create the required Oracle schemas in the database using the Repository Creation Utility (RCU). See Section 10.5, "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU."

10.2 Verifying the Database Requirements for an Enterprise Deployment

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

- Section 10.2.1, "Databases Required"
- Section 10.2.2, "Database Host Requirements"
- Section 10.2.3, "Database Versions Supported"
- Section 10.2.4, "Patch Requirements for Oracle Database 11g (11.2.0.2.0)"
- Section 10.2.5, "Oracle Database Minimum Requirements"

10.2.1 Databases Required

Oracle Identity and Access Management data can be placed into one or more databases. Table 10–1 shows a single database with multiple database services accessing it. If desired, you can configure these services to point to a different database if necessary. Utilizing separate database services at the start allows data to be segregated into different databases at a later date, with minimum application configuration.

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

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

Table 10–1 Mapping between Databases and Schemas

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

The following sections apply to all the databases listed in Table 10–1.

10.2.2 Database Host Requirements

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

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

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

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

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

10.2.3 Database Versions Supported

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

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

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

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

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

10.2.4 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

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

Table 10–2 lists the patches required for Oracle Identity Manager configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 10–2 Required Patches for Oracle Database 11g (11.2.0.2.0)

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

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

Note:

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

10.2.5 Oracle Database Minimum Requirements

The Oracle Database must meet some minimum requirements.

10.2.5.1 General Database Characteristics

- Character Set–The character set must be Unicode compliant, for example: AL32UTF8.

- Database Options–The following database options must be installed into the database:
  - Oracle JVM
  - Oracle Text
- Database Views–The following Database view must be created on the database:
  - XAVIEWS
- Database Packages–The following Database package must exist in the database:
  - DBMS_SHARED_POOL

10.2.5.2 Minimum Initialization Parameters

The databases must have the following minimum initialization parameters defined:

Table 10–3 Minimum Initialization Parameters for Oracle Databases

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

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

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

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

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

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

10.3 Installing the Database for an Enterprise Deployment

Install and configure the database repository as follows.

Oracle Clusterware

- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- For 11*g* Release 1 (11.1), see *Oracle Clusterware Installation Guide*.
- When you run the installer, select the **Configure Automatic Storage Management** option in the **Select Configuration** screen to create a separate Automatic Storage Management home.

Oracle Real Application Clusters

- For 11*g* Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

Oracle Real Application Clusters Database

Create a Real Applications Clusters Database with the following characteristics:

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

10.4 Creating Database Services

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

- Section 10.4.1, "Creating Database Services for 11.2.x Databases"
- Section 10.4.2, "Database Tuning"

10.4.1 Creating Database Services for 11.2.x Databases

Use `srvctl` to create the database services for the components in your topology. The lists of services to be created are listed in Table 10–1, " Mapping between Databases and Schemas".

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

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

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

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

Option	Argument
-z	Failover retries (integer)

2. Start the Service using `srvctl start service`

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

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

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

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

   ```
   srvctl config service -d iamdb -s OAMEDG.mycompany.com
   Service name: OAMEDG.mycompany.com
   Service is enabled
   Server pool: IAMDB_OAMEDG.mycompany.com
   Cardinality: 2
   Disconnect: false
   Service role: PRIMARY
   Management policy: AUTOMATIC
   DTP transaction: false
   AQ HA notifications: false
   Failover type: SELECT
   Failover method: NONE
   TAF failover retries: 0
   TAF failover delay: 0
   Connection Load Balancing Goal: LONG
   Runtime Load Balancing Goal: NONE
   TAF policy specification: NONE
   Edition:
   Preferred instances: iamdb1,iamdb2
   Available instances:
   ```

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

10.4.2 Database Tuning

The database parameters defined in Section 10.2.5.2, "Minimum Initialization Parameters" are only a guide. You might need to perform additional tuning after the system is in use. For more information, see *Database Performance Tuning Guide*.

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

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

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

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

1. Start RCU by issuing this command:

   ```
   RCU_ORACLE_HOME/bin/rcu &
   ```

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

3. On the Create Repository screen, select the **Create** operation to load component schemas into a database. Then click **Next**.

4. On the Database Connection Details screen, provide the information required to connect to an existing database. For example:

   Database Type: `Oracle Database`

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

     Use the service names for the components you will select from the table in Step 6.
   - **Username:** `sys`
   - **Password:** The sys user password
   - **Role:** `SYSDBA`

   Click **Next**.

5. On the Check Prerequisites screen, click `OK` after the prerequisites have been validated.

6. On the Select Components screen, provide the following values:

   Create a New Prefix: Enter a prefix to be added to the database schemas. Note that all schemas are required to have a prefix. See Table 10–1, " Mapping between Databases and Schemas" or the following table for RCU prefixes.

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

RCU Prefix	Product	RCU Option	Comments
EDGIAD	Oracle Platform Security Services for IAMAccessDomain	AS Common Schemas–Oracle Platform Security Service	Audit and Metadata Services are also selected.
EDGIAD	Oracle Access Management Access Manager	Identity Management–Oracle Access Manager	Audit Services will also be selected.

RCU Prefix	Product	RCU Option	Comments
EDGIAD	Oracle Adaptive Access Manager	Oracle Identity Management–Oracle Adaptive Access Manager	If required.
EDGIGD	Oracle Platform Security Services for IAMGovernanceDomain	AS Common Schemas–Oracle Platform Security Service	Audit and Metadata Services are also selected.
EDGIGD	Oracle Identity Manager	Identity Management–Oracle Identity Manager	Metadata Services, SOA infrastructure, and User Messaging will also be selected.

Click **Next**.

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

- Be sure to install the correct schemas in the correct database.
- You might have to run the RCU more than once to create all the schemas for a given topology.
- Table 10–1 in this chapter provides the recommended mapping between the schemas and their corresponding databases. Refer to this table to ensure that the correct details are entered in this screen.

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. The deployment wizard requires that all passwords for a given prefix be the same.

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

    Click **Close** to exit.

10.6 Exadata and SDP Connections

If your Database is on an Exadata machine, you can opt to connect to the database either through TCP or SDP. Even if using SDP, a TCP connection to the database must exist as the TCP connection is used for the provisioning process. Later, during post-provisioning, the TCP connection can optionally be changed to an SDP connection. The following two sub-sections describe prerequisites for the SDP connection.

10.6.1 Create an SDP Infiniband Listener

Create an SDP listener on the Exadata machine by following the instructions in "Configuring SDP InfiniBand Listener for Exalogic Connections" in *Oracle Fusion Middleware Exalogic Enterprise Deployment Guide, Release EL X2-2 and EL X3-2.*

10.6.2 Disable APM

As described in My Oracle Support Note 1588546.1, having SDP and APM enabled can result in database hangs. As a result, Oracle recommends disabling APM on both the Exalogic and Exadata nodes.

To disable APM:

1. Add the argument `sdp_apm_enable=0` to the infiniband options in the file `/etc/modprobe.conf`.

   After editing, the entry should look like this:

   ```
   options ib_sdp sdp_zcopy_thresh=0 recv_poll=0 sdp_apm_enable=0
   ```

2. Reload the `ib_sdp` driver:

   ```
   modprobe -r ib_sdp
   modprobe ib_sdp
   ```

3. Validate that change by running the following command:

   ```
   [root@xxx03cn05 ~]# cat /sys/module/ib_sdp/parameters/sdp_apm_enable
   0
   [root@xxx03cn05 ~]#
   ```

   The result should be `0`.

10.7 Backing up the Database

After you have prepared your database, back it up as described in Section 20.5.3.3, "Backing Up the Database."

11

Preparing for Deployment

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

This chapter contains the following topics:

11.1 Assembling Information for Identity and Access Management Deployment

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

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

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

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

In addition to the host names, you may see some of the hosts with an EXT suffix (generally used in the OHS topology). The EXT suffix is used to denote that the external EoIB network interface is used.

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

In certain circumstances you may see hosts with a suffix of EXTVHN. In this scenario this suffix is referring to a virtual hostname configured on the EoIB network.

Notes:

- Do not use host names that contain the hyphen (**-**) character. See Section 20.10.2.1, "Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute."
- Do not use privileged ports (< 1024) for the Identity and Access Management deployment.

Table 11–1 Hosts–Virtual Exalogic

Description	Variable	Documented Value	Customer Value
Access Management Host 1	*OAMHOST1*	`OAMHOST1.mycompany.com`	
Access Management Host 2	*OAMHOST2*	`OAMHOST2.mycompany.com`	
Identity Governance Host 1	*OIMHOST1*	`OIMHOST1.mycompany.com`	
Identity Governance Host 2	*OIMHOST2*	`OIMHOST2.mycompany.com`	
Directory Host 1	*LDAPHOST1*	`OAMHOST1.mycompany.com`	
Directory Host 2	*LDAPHOST2*	`OAMHOST2.mycompany.com`	
First Web Tier host	*WEBHOST1*	`OAMHOST1.mycompany.com`	
Second Web Tier host	*WEBOST2*	`OAMHOST2.mycompany.com`	

Table 11–2 Hosts–Physical Exalogic

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

Table 11–3 Hosts–External OHS

Description	Variable	Documented Value	Customer Value
Access Management Host 1	*OAMHOST1*	`IAMHOST1EXT.mycompany.com`	
Access Management Host 2	*OAMHOST2*	`IAMHOST2EXT.mycompany.com`	
Identity Governance Host 1	*OIMHOST1*	`IAMHOST1EXT.mycompany.com`	
Identity Governance Host 2	*OIMHOST2*	`IAMHOST2EXT.mycompany.com`	
Directory Host 1	*LDAPHOST1*	`IAMHOST1EXT.mycompany.com`	
Directory Host 2	*LDAPHOST2*	`IAMHOST2EXT.mycompany.com`	
First Web Tier host	*WEBHOST1*	`OHSHOST1.mycompany.com`	
Second Web Tier host	*WEBHOST2*	`OHSHOST2.mycompany.com`	

Table 11–4 Installation Locations

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

Table 11–5 Ports

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

Table 11–6 Virtual Hosts

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

Table 11–6 (Cont.) Virtual Hosts

Description	Variable	Documented Value	Customer Value
Second Oracle Identity Manager Server virtual host	*OIMHOST2VHN*	`OIMHOST2VHN.mycompany.com`	
First SOA Server virtual host	*SOAHOST1VHN*	`SOAHOST1VHN.mycompany.com`	
Second SOA Server virtual host	*SOAHOST2VHN*	`SOAHOST2VHN.mycompany.com`	

Table 11–7 Database Information

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

Table 11–8 LDAP

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

Table 11–9 Load Balancer

Description	Variable	Documented Value	Customer Value
Load Balancer end point used to access the IAMAccessDomain Administration functions	*IAD_DOMAIN_ADMIN_LBRVHN*	`IADADMIN.mycompany.com`	
Load Balancer end point used to access the IAMGovernanceDomain Administration functions	*IGD_DOMAIN_ADMIN_LBRVHN*	`IGDADMIN.mycompany.com`	
Load Balancer Administration Port	*HTTP_PORT*	`80`	
Load Balancer Administration Port is SSL?		`No`	
Load Balancer Internal Callbacks Virtual Host Name	*IAM_INTERNAL_LBRVHN*	`IDMINTERNAL.mycompany.com`	
Load Balancer Internal Callbacks Port	*IAM_INTERNAL_PORT*	`7777`	
Load Balancer SSL Port	*HTTP_SSL_PORT*	`443`	
Load Balancer ID Store Virtual Host Name	*LDAP_IDSTORE_NAME*	`IDSTORE.mycompany.com`	

Table 11–9 (Cont.) Load Balancer

Description	Variable	Documented Value	Customer Value
Load Balancer ID Store Port	*LDAP_LBR_PORT*	1489	
Load Balancer ID Store SSL Port	*LDAP_LBR_SSL_PORT*	1636	
SSO main application entry point	*IAM_LOGIN_LBRVHN*	SSO.mycompany.com	

Table 11–10 Email Server (Optional)

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

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

Table 11–11 Users

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

Table 11–12 OAM

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

Table 11–13 Oracle Traffic Director

Description	Variable	Documented Value	Customer Value
OTD Node Port	*OTD_NODE_PORT*	8900	
OTD Admin port	*OTD_ADMIN_PORT*	8800	
OTD Admin user	*OTDADMIN*	otdadmin	

11.2 Creating an Oracle Identity and Access Management Software Repository

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

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

```
REPOS_HOME/installers/rcu
```

11.3 Oracle Traffic Director

Oracle Traffic Director and Oracle WebGate for Traffic Director are not supplied as part of the software repository.

You must download these separately. It is recommended that you extract these to the Software Repository for consistency.

Extract OTD to `REPOS_HOME/installers/otd`

Extract OTD WebGate to `REPOS_HOME/installers/webgate_otd`

11.4 Verifying Java

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

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

Set `JAVA_HOME` to: *JAVA_HOME*

Run these commands:

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

11.5 Installing the IAM Deployment Wizard

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

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

```
REPOS_HOME/installers/idmlcm/Disk1
```

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

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

Then proceed as follows:

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

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

   In the **Operating System Group ID** field, select the group whose members you want to grant access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue.

   The **Inventory Location Confirmation** dialog prompts you to run the `*inventory_directory*/createCentralInventory.sh` script as `root` to create the `/etc/oraInst.loc` file. This file is a pointer to the central inventory and must be present for silent installations. It contains two lines:

   ```
   inventory_loc=path_to_central_inventory
   ```

   ```
   inst_group=install_group
   ```

   The standard location for this file is `/etc/oraInst.loc`, but it can be created anywhere. If you create it in a directory other than `/etc`, you must include the `-invPtrLoc` argument and enter the location of the inventory when you run the Identity and Access Management Deployment Wizard or the `runIAMDeployment` script.

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

   Click **OK** to continue.

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

4. On the Specify Install Location screen, enter the following information:

   a. Oracle Middleware Home - This is the parent directory of the directory where the Identity and Access Management Deployment Wizard will be installed. This must be on shared storage for example:

      ```
      /u01/lcm/tools
      ```

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

      ```
      idmlcm
      ```

   Click **Next**.

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

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

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

11.6 Checking Port Availability

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

To do this, perform the following steps:

1. Log on to the machine that the component will run on.

2. Check that no process is running on that port using the following command:

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

   where *`port`* is the port number you are checking for. See ports listed in Table 11–5.

For example, for Oracle HTTP server the command is:

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

For a full list of the default ports, see Chapter 4–3, " Ports Used in the Exalogic Reference Topology."

12

Installing and Configuring Oracle Traffic Director for an Enterprise Deployment

This chapter describes how to install and configure Oracle Traffic Director for an Exalogic enterprise deployment.

This chapter contains the following sections:

12.1 Overview of Installing and Configuring Oracle Traffic Director for an Enterprise Deployment

Oracle Traffic Director is a software load balancer for load balancing HTTP/S and TCP traffic to servers in the back-end. These back-end servers, which are referred to as origin servers within Oracle Traffic Director, can be application servers, web servers, or LDAP servers.

Installing and configuring Oracle Traffic Director for an enterprise deployment involves performing the steps shown in Table 12–1.

Table 12–1 Overview of Installing and Configuring Oracle Traffic Director for an Enterprise Deployment

Task	Description	More Information
Review Oracle Traffic Director prerequisites.	For example, be sure that you have set up the required virtual IP addresses, that the user account has root permission on the storage appliance, and that you have already created the initial Oracle WebLogic Server domain for the Oracle Identity Management topology.	"Prerequisites" in the *Oracle Traffic Director Installation Guide*
Install the Oracle Traffic Director software.	You install the software using the directories and mount points you created in Section 7.4.4, "Recommended Directory Locations."	Section 12.2, "Installing Oracle Traffic Director on WEBHOST1 and WEBHOST2"
Create and start an Oracle Traffic Director Administration Server.	The Oracle Traffic Director administration server hosts the administration console and command-line interface, through which you can create Oracle Traffic Director configurations, deploy them as instances on administration nodes, and manage the instances.	Section 12.3, "Creating and Starting the Traffic Director Administration Server"
Verify the installation.	Be sure that the installation was successful before you continue configuring the environment.	"Verifying the Installation" in the *Oracle Traffic Director Installation Guide*
Register WEBHOST2 as administration node.	This ensures that Oracle Traffic Director is up and running on both WEBHOST1 and WEBHOST2.	Section 12.4, "Register WEBHOST2 with the Administration Node"
Create a configuration	The configuration should route requests from the Oracle Traffic Director instances to the managed servers in the Oracle WebLogic Server domain. The configuration should also define the required origin-server pools to which requests should be routed.	Section 12.5, "Creating a Configuration"
Start the Oracle Traffic Director instances	Start the instances on WEBHOST1 and WEBHOST2, based on the configuration you created earlier in this procedure.	Section 12.6, "Starting, Stopping, and Restarting Oracle Traffic Director"
Define the virtual servers.	Define the virtual servers required for accessing the various management tools and login screens for the topology.	Section 12.7, "Defining the Required Oracle Traffic Director Virtual Servers for an Enterprise Deployment"
Create Routes	Adding routes allows a virtual server to direct requests to different server pools depending on what is contained within the URI.	Section 12.8, "Creating Routes"

Table 12–1 (Cont.) Overview of Installing and Configuring Oracle Traffic Director for an Enterprise

Task	Description	More Information
Enable SSL Passthrough for sso.mycompany.com	Perform extra configuration steps to ensure that any application redirects occur correctly.	Section 12.9, "Enabling SSL Passthrough for sso.mycompany.com"
Deploy and test the configuration.	Deploy the configuration and test the virtual server URLs to be sure you have configured the Oracle Traffic Director instances successfully.	Section 12.11, "Deploying the Configuration and Testing the Virtual Server Addresses"
Create an active-passive failover group.	Create a failover group to ensure that requests will continue to be served if WEBHOST1 or WEBHOST2 become unavailable.	Section 12.12, "Creating a Failover Group for Virtual Hosts"

12.2 Installing Oracle Traffic Director on WEBHOST1 and WEBHOST2

This section describes how to install Oracle Traffic Director software.

> **Note:** Be sure that you are not logged in as root user before installing or performing any action on Oracle Traffic Director.

> **Note:** Be sure to verify you have obtained all required patches. For more info, see Section 3.7.4, "Applying Patches and Work-arounds."

To install Oracle Traffic Director:

1. Extract the contents of the installer zip file to a directory on WEBHOST1.
2. Change directory to the `Disk1` subdirectory in the directory in which you unzipped the installer.
3. Run the following command:

   ```
   ./runInstaller
   ```

4. Follow the instructions on the screen to install the software.

   When the Specify Installation Location screen appears, enter the value of the *OTD_ORACLE_HOME* variable in the **Oracle Home Directory** field.

   The recommended directory location for the *OTD_ORACLE_HOME* is listed in Table 7–3, " Private Storage Directories"

   If you need help with any of the other options on the installer screens, click **Help**, or refer to "Installing Oracle Traffic Director in Graphical Mode" in the *Oracle Traffic Director Installation Guide*.

5. Repeat steps 1 through 5 on WEBHOST2.

12.3 Creating and Starting the Traffic Director Administration Server

After you install Oracle Traffic Director on WEBHOST1 and WEBHOST2, you can then create an Oracle Traffic Director administration server.

For more information, see "Managing the Administration Server" in the *Oracle Traffic Director Administrator's Guide*

To create the Oracle Traffic Director administration server on WEBHOST1 run the **tadm** command from the *OTD_ORACLE_HOME*/bin directory, as follows:

1. On WEBHOST1 enter the following command:

   ```
   OTD_ORACLE_HOME/bin/tadm configure-server --port=OTD_ADMIN_PORT \
   --user=otdadmin --instance-home=OTD_ORACLE_INSTANCE --host=OTDADMINVHN
   --server-user=root
   ```

   Where:

   - *OTD_ORACLE_HOME* the Oracle Home location you entered in the Oracle Traffic Director installer.
   - *OTD_ORACLE_INSTANCE* is the recommended value listed in Table 7–3, " Private Storage Directories".
   - OTDADMINVHN is the virtual host name to be used for the Oracle Traffic Director administration server and console.

   For example:

   ```
   OTD_ORACLE_HOME/web/bin/tadm configure-server --port=8800 --user=otdadmin \
   --instance-home=/u02/private/oracle/config/otd1
   --host=OTDADMINVHN.mycompany.com
   ```

   > **Note:** If you want to run Oracle Traffic Director as the root user, which is necessary if you want Oracle Traffic Director to work using ports <1024, you must add the following additional parameter to the command:
   >
   > ```
   > --server-user=root
   > ```

2. Enter the administrator password.

   You will later use this password to log in to the Oracle Traffic Director administration console.

   A prompt to re-enter the administrator password is displayed, as follows:

   ```
   Please enter admin-user-password again>
   ```

3. Confirm the administrator password by entering it again.

   An Administration Server instance of Oracle Traffic Director is created and deployed on the local host in a directory named admin-server within the *OTD_ORACLE_INSTANCE* directory that you specified in step 1.

4. Start the Administration Server by running the following command on WEBHOST1:

   ```
   WEB_INSTANCE_HOME/admin-server/bin/startserv
   ```

   If you want the server to run as root, start it as root.

5. Log in to the Administration Server using the following URL:

   ```
   https://OTDADMINVHN:8800
   ```

where 8800 is *OTD_ADMIN_PORT*.

Use the password provided above and verify that you can see the Oracle Traffic Director main page.

12.4 Register WEBHOST2 with the Administration Node

This section assumes you have installed Oracle Traffic Director, started the Administration Server, and verified the installation.

WEBHOST1 and WEBHOST2 have IP over InfiniBand (IPoIB) addresses. For example, 192.168.10.5 and 192.168.10.6.

You can now register WEBHOST2 with the Oracle Traffic Director Administration Server using the **tadm** command from the *OTD_ORACLE_HOME*/bin directory, as follows:

1. On the WEBHOST2, run the configure-server command to register the host with the remote Administration Server as an administration node.

```
./tadm configure-server --user=otdadmin --port=OTD_ADMIN_PORT
--host=OTDADMINVHN \
--admin-node --node-port=OTD_NODE_PORT --instance-home=OTD_ORACLE_INSTANCE
--node-host=WEBHOST2 --server-user=root
```

Where:

- *OTD_ORACLE_HOME* is the path to the Oracle Traffic Director Oracle home on WEBHOST2.
- *WEB_INSTANCE_HOME* is the recommended directory path listed in Table 7–3, " Private Storage Directories"
- *node-host* is the name of the machine that this instance is running on (IAMHOST1, IAMHOST2, or WEBHOST2).

For example:

```
./tadm configure-server --user=otdadmin --port=8800 --host=OTDADMINVHN
--admin-node \
--node-port=8900 --instance-home=/u02/private/oracle/config/instances/otd2
--node-host=WEBHOST2
```

> **Note:** If you want to run Oracle Traffic Director as the root user, which is necessary if you want Oracle Traffic Director to work using ports <1024, you must add the following additional parameter to the command:
>
> ```
> --server-user=root
> ```

For more information, see "configure-server" in the *Oracle Traffic Director Command-Line Reference* or use the configure-server --help command to see an explanation of the command line options.

The following prompt appears after you run configure-server command:

```
This command creates an Administration Node and register it with the following
remote Administration Server: https://WEBHOST1.mycompany.com
```

```
Enter admin-user password>
```

2. Enter the admin-user password for the Oracle Traffic Director Administration Server.

   The `configure-server` command attempts to connect to the remote administration server by using the specified administration server host, port, user, and password. The Administration Server on WEBHOST1 must be up and running.

   If this is the first time that the host on which you are creating the administration node is attempting to connect to the administration server, the server certificate of the administration server is displayed.

3. Enter `y` to trust the certificate.

   The following message is displayed:

   ```
   OTD-70215 The administration node has been configured successfully.
   The node can be started by executing:
   OTD_ORACLE_INSTANCE/admin-server/bin/startserv
   ```

4. Start the Oracle Traffic Director Server by running the following command on WEBHOST2:

   ```
   WEB_INSTANCE_HOME/admin-server/bin/startserv
   ```

   If you want the server to run as `root`, start it as `root`.

After you start the administration node, you can create instances of Oracle Traffic Director configurations on the administration node. Note that on each administration node, you can create only one instance of a configuration.

12.5 Creating a Configuration

The next step in installing and configuring Oracle Traffic Director for an enterprise deployment is to create a configuration that will route requests to a server pool that consists of the managed servers in your Oracle WebLogic Server domain.

When creating a new configuration, you are required to provide the host and port information for the origin server, which in turn automatically creates (and names) an origin-server pool called **origin-server-pool-1**. This is the default origin-server pool and this pool can be found when you click the Server Pools option in the administration console. You cannot rename the default origin-server pool.

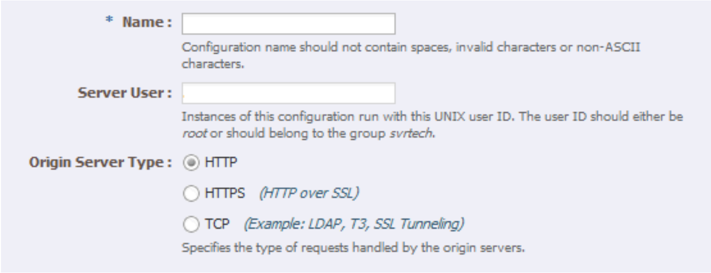
To create a configuration named IAM by using the administration console:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs."

2. In the Common Tasks pane, click **New Configuration**.

   The New Configuration wizard starts.

Figure 12–1 New Configuration Wizard



* Name :

Configuration name should not contain spaces, invalid characters or non-ASCII characters.

Server User :

Instances of this configuration run with this UNIX user ID. The user ID should either be *root* or should belong to the group *svrtech*.

Origin Server Type : ● HTTP

○ HTTPS *(HTTP over SSL)*

○ TCP *(Example: LDAP, T3, SSL Tunneling)*

Specifies the type of requests handled by the origin servers.

3. In the Step 1 Configuration Information screen, enter the following information:

   - **Name:** `sso.mycompany.com`
   - **Server User:** `oracle` (or `root`, if you want the server instances to run as `root`).
   - **Origin Server Type**: Make sure **HTTP** is selected.

   Click **Next**.

4. On the Listener Information Screen set the port to a dummy port, for example: 6666. This port should not be the port that you want to eventually use, for example: 7777 (*`WEB_HTTP_PORT`*). Setting this port to a dummy value is required so that the Oracle Traffic Director configuration does not interfere with the provisioning process. After provisioning the port will be updated to the correct value.

   Accept the other default values and click **Next.**

5. In the Step 3 Server Pool Information screen:

   a. In the **Origin Servers: Host:** field, enter *OAMHOST1*`.mycompany.com`, the port `14100` (*`OAM_PORT`*), and click **Add Server**.

   b. Enter *OAMHOST2*`.mycompany.com` and port `14100`, click **Add Server** and click **Next**.

6. In the Step 4 Deployment Information screen, select the **Administration Server** and *WEBHOST2* and click **Next**.

   The Review screen appears.

7. Review the information and click **Create Configuration**.

   The Results screen appears.

   After the configuration is created, the Results screen of the New Configuration wizard displays a message confirming successful creation of the configuration. If you chose to create instances of the configuration, then a message confirming successful creation of the instances is also displayed.

8. Click **Close** on the Results screen.

   In the New Configuration wizard, if you chose not to create an instance of the configuration, the message **Undeployed Configuration** is displayed, indicating that the configuration that you just created is yet to be deployed.

12.6 Starting, Stopping, and Restarting Oracle Traffic Director

To start and stop Oracle Traffic Director instances see Section 20.1.5, "Starting the Oracle Traffic Director Instances"

12.7 Defining the Required Oracle Traffic Director Virtual Servers for an Enterprise Deployment

Create and configure the virtual servers for the Oracle Traffic Director configuration. In this section you create the following Oracle Traffic Director virtual servers for your Oracle Identity and Access Management deployment. If External Oracle HTTP Servers are being used then several of these virtual servers should not be enabled on the Oracle Traffic Director.

Table 12–2 Defining Virtual Servers

Virtual Server	Purpose	Creating the Virtual Server	Required with OHS
sso.mycompany.com	Acts as the access point for all HTTP traffic that gets directed to the single sign on services.	This virtual server is created through administration console in Section 12.7.2, "Creating Virtual Servers.".	No
iadadmin.mycompany.com	Acts as the access point for all internal HTTP traffic that gets directed to the administration services.	This virtual server is created through administration console in Section 12.7.2, "Creating Virtual Servers.".	No
idstore.mycompany.com	Acts as the access point for all Identity Store LDAP traffic.	This virtual server is created through administration console in Section 12.7.2, "Creating Virtual Servers.".	Yes
idminternal.mycompany.com	Acts as a load balancer, routing requests to SOA servers on *IAMHOST1* and *IAMHOST2*.	This virtual server is created when you configure the TCP Proxy for OUD in Section 12.7.3, "Creating a TCP Proxy and Listener for idstore.mycompany.com.".	Yes
igdadmin.mycompany.com	Acts as the access point for all internal HTTP traffic that gets directed to the Administration services in the IAMGovernanceDomain	The virtual server is created through the administration console in Section 12.7.2, "Creating Virtual Servers.".	No

To create and configure virtual servers using the administration console complete the steps in the following sections:

- Section 12.7.1, "Creating an Origin-Server Pool"
- Section 12.7.2, "Creating Virtual Servers"
- Section 12.7.3, "Creating a TCP Proxy and Listener for idstore.mycompany.com"

12.7.1 Creating an Origin-Server Pool

A server pool is a group of one or more virtualization hosts with the same processor architecture that have access to the same virtual and physical networks, and storage resources. Server pools provide load balancing, high availability capabilities, and sharing of some resources for all members of the pool.

In this section, create the Oracle Traffic Director origin-server pools listed in Table 12–5.

Table 12–3 Origin-Server Pools and Origin Servers for Physical Exalogic

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.mycompany.com	7001 (*IAD_WLS_PORT*)
igdadmin-pool	HTTP	IGDADMINVHN.mycompany.com	7101 (*IGD_WLS_PORT*)
oud-pool	TCP	IAMHOST1.mycompany.com, IAMHOST2.mycompany.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHN.mycompany.com, OIMHOST2VHN.mycompany.com	14000 (*OIM_PORT*)
origin-server-pool-1	HTTP	IAMHOST1.mycompany.com, IAMHOST2.mycompany.com	14100 (*OAM_PORT*)
soa-pool	HTTP	SOAHOST1VHN.mycompany.com, SOAHOST2VHN.mycompany.com	8001 (*SOA_PORT*)
oaam-pool[1]	HTTP	IAMHOST1.mycompany.com, IAMHOST2.mycompany.com	14300 (*OAAM_PORT*)
oaam-admin-pool	HTTP	IAMHOST1.mycompany.com, IAMHOST2.mycompany.com	14200 (*OAAM_ADMIN_PORT*)

[1] oaam-pool and oaam-admin-pool are only required if the topology includes OAAM.

Table 12–4 Origin-Server Pools and Origin Servers for External OHS Servers

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.mycompany.com	7001 (*IAD_WLS_PORT*)
igdadmin-pool	HTTP	IGDADMINVHN.mycompany.com	7101 (*IGD_WLS_PORT*)
oud-pool	TCP	IAMHOST1EXT.mycompany.com, IAMHOST2EXT.mycompany.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHNEXT.mycompany.com, OIMHOST2VHNEXT.mycompany.com	14000 (*OIM_PORT*)
origin-server-pool-1	HTTP	IAMHOST1EXT.mycompany.com, IAMHOST2EXT.mycompany.com	14100 (*OAM_PORT*)
soa-pool	HTTP	SOAHOST1VHN.mycompany.com, SOAHOST2VHN.mycompany.com	8001 (*SOA_PORT*)
oaam-pool[1]	HTTP	IAMHOST1EXT.mycompany.com, IAMHOST2EXT.mycompany.com	14300 (*OAAM_PORT*)
oaam-admin-pool	HTTP	IAMHOST1EXT.mycompany.com, IAMHOST2EXT.mycompany.com	14200 (*OAAM_ADMIN_PORT*)

[1] oaam-pool and oaam-admin-pool are only required if the topology includes OAAM.

Table 12–5 Origin-Server Pools and Origin Servers for Virtual Exalogic

Origin-Server Pool	Origin Server Type	Origin Servers	Port
iadadmin-pool	HTTP	IADADMINVHN.mycompany.com	7001 (*IAD_WLS_PORT*)
igdadmin -pool	HTTP	IGDADMINVHN.mycompany.com	7101 (*IGD_WLS_PORT*)
oud-pool	TCP	OAMHOST1.mycompany.com, OAMHOST2.mycompany.com	1389 (*LDAP_PORT*)
oim-pool	HTTP	OIMHOST1VHN.mycompany.com, OIMHOST2VHN.mycompany.com	14000 (*OIM_PORT*)
origin-server-pool-1	HTTP	OAMHOST1.mycompany.com, OAMHOST2.mycompany.com	14100 (*OAM_PORT*)
soa-pool	HTTP	SOAHOST1VHN.mycompany.com, SOAHOST2VHN.mycompany.com	8001 (*SOA_PORT*)
oaam-pool[1]	HTTP	OAMHOST1.mycompany.com, OAMHOST2.mycompany.com	14300 (*OAAM_PORT*)
oaam-admin-pool	HTTP	OAMHOST1.mycompany.com, OAMHOST2.mycompany.com	14200 (*OAAM_ADMIN_PORT*)

[1] oaam-pool and oaam-admin-pool are only required if the topology includes OAAM.

> **Note:** The `oim-server-pool-1` is created automatically for you when you created the configuration.

To create an origin-server pool:

1. Log in to the Administration Console using the following URL:

   ```
   https://OTDADMINVHN:OTD_ADMIN_PORT
   ```

   where *OTD_ADMIN_PORT* is defined in Section 11.1, "Assembling Information for Identity and Access Management Deployment."

2. Click the **Configurations** button that is situated at the upper left corner of the page.

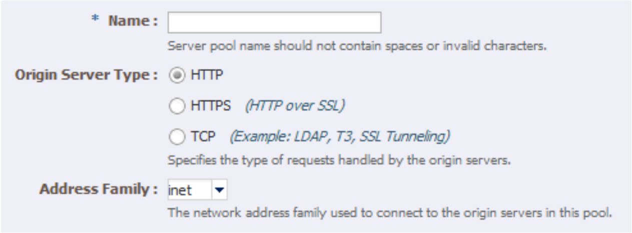
   A list of the available configurations is displayed.

3. Select the configuration for which you want to create a server pool. For example: for example, `sso.mycompany.com`.

4. In the **Common Tasks** pane, click **New Server Pool**.

   The New Origin-Server Pool wizard starts.

Figure 12–2 New Origin-Server Pool Wizard



* Name :

Server pool name should not contain spaces or invalid characters.

Origin Server Type : ● HTTP

○ HTTPS *(HTTP over SSL)*

○ TCP *(Example: LDAP, T3, SSL Tunneling)*

Specifies the type of requests handled by the origin servers.

Address Family : inet ▾

The network address family used to connect to the origin servers in this pool.

5. Enter the following information in the Server Pool Information screen:
   - **Name:** Name of the server pool. For example, `oim-pool`
   - **Origin Server Type**: The type of requests the pool handles. For example, `HTTP`.

   Click **Next**.
6. Enter the following information in the Origin Server Information screen:
   - **Origin Server Host**: `OIMHOST1VHN.mycompany.com`
   - **Port**: `14000` (*`OIM_PORT`*)

   Click **Add Server**.
7. Enter the information for any other servers. For example:
   - **Origin Server Host**: `OIMHOST2.mycompany.com`
   - **Port**: `14000` (*`OIM_PORT`*)

   Click **Next**.

   Review the information on the Review screen. If the information is correct, click **Create Server Pool**.
8. For each HTTP pool that was created and has more than one origin server, perform the additional configuration steps:

   a. Click on the newly create server pool name, for example `oim-pool`.

      The pool properties appear.

   b. Expand the **Advanced Settings**.

   c. Enable the check box **Dynamic Discovery**

      This ensures that any new cluster members added at a later date are automatically added to the OTD server pool without you having to add them manually, although it is still good practice.

      Note: You cannot use Dynamic Discovery for the OUD origin server pool (oud-pool)

   d. Click **Save**.
9. Click **Close** on the Results screen.
   - The details of the origin-server pool that you just created are displayed on the Origin-Server Pools page.
   - In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking **Deploy Changes**, or you can do so later after making further changes

as described in Section 12.11, "Deploying the Configuration and Testing the Virtual Server Addresses."

10. Repeat these steps for the origin-server pool listed in Table 12–3.

12.7.2 Creating Virtual Servers

Create virtual servers using the information in Table 12–7, " Routes and Conditions".

Table 12–6 Virtual Server Information

Name	Host	Pool
sso.mycompany.com	sso.mycompany.com	origin-server-pool-1
iadadmin.mycompany.com	iadadmin.mycompany.com	iadadmin-pool
igdadmin.mycompany.com	igdadmin.mycompany.com	igdadmin-pool
idminternal.mycompany.com	idminternal.mycompany.com	oim-pool

> **Note:** The `sso.mycompany.com` virtual server is created automatically when you created the configuration.

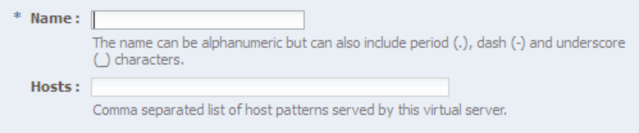
To create a virtual server using the administration console:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button that is situated at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to create a virtual server, for example `sso.mycompany.com`.
4. In the Common Tasks pane, click **New Virtual Server**.

   The New Virtual Server wizard starts.

Figure 12–3 New Virtual Server Wizard



* Name :

The name can be alphanumeric but can also include period (.), dash (-) and underscore (_) characters.

Hosts :

Comma separated list of host patterns served by this virtual server.

5. On the Virtual Server Information Page enter the following information:
   - **Name**: The name describing the virtual server. For example, `sso.mycompany.com`
   - **Host**: The name in the DNS/Hosts which is used to access this virtual server. For example, `sso.mycompany.com`

   Click **Next**.
6. On the HTTP Listener Information screen, select the existing Listener.

   Click **Next**.

7. On the server Pool Information Screen, enter the following information:

   - **Select**: Select a pool of origin servers.
   - **Name**: Select the name of one of the server pools you created in 12.7.1 , "Creating an Origin-Server Pool".

   Click **Next**.

8. Review the supplied information in the Review screen and click **Create Virtual Server**.

9. Repeat steps 4-6 for each virtual server in Table 12–6.

12.7.3 Creating a TCP Proxy and Listener for idstore.mycompany.com

Create a TCP Proxy using the administration console.

To create a TCP Proxy:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":

2. Click the **Configurations** button that is situated at the upper left corner of the page.

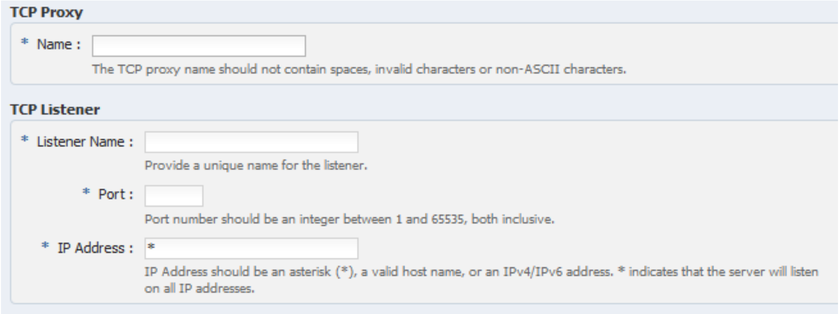
   A list of the available configurations is displayed.

3. Select the configuration for which you want to create a TCP Proxy, for example `sso.mycompany.com`.

4. In the Common Tasks pane, click **New TCP Proxy**.

   The New TCP Proxy wizard starts.

Figure 12–4 New TCP Proxy Wizard



TCP Proxy

* Name :

The TCP proxy name should not contain spaces, invalid characters or non-ASCII characters.

TCP Listener

* Listener Name :

Provide a unique name for the listener.

* Port :

Port number should be an integer between 1 and 65535, both inclusive.

* IP Address : *

IP Address should be an asterisk (*), a valid host name, or an IPv4/IPv6 address. * indicates that the server will listen on all IP addresses.

5. In the Step 1: TCP Proxy Information screen, enter the following information and click **Next**:

   - **Name**: `idstore.mycompany.com`
   - **Listener Name**: `listener-oud`
   - **Port**: `1489` (*`LDAP_LBR_PORT`*)

   > **Note:** If OUD and OTD are running on the same host, the port used by OTD to route requests to OUD must be a different port from the OUD port

   - In the **IP Address** field, enter `*`.

6. In the Step 2: Server Pool Information screen, click **Select a pool of origin servers**.
7. In the drop-down list, select **oud-pool** and click **Next**.

   The Review screen appears.
8. Review the details and click **Create TCP Proxy**.
9. Click **Close** on the Results screen.
   - The details of the TCP Proxies that you just created are displayed on the TCP proxies page.
   - In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking **Deploy Changes**, or you can do so later after making further changes, as described in Section 12.11, "Deploying the Configuration and Testing the Virtual Server Addresses."

12.8 Creating Routes

> **Note:** This section is only relevant when Oracle Traffic Director is used as a web server.

Routes are similar to an Oracle HTTP location directives. Any requests received for a specific URI inside a virtual server are directed to the appropriate server pool. Adding routes allows a virtual server to direct requests to different server pools depending on what is contained within the URI.

Create the routes listed in Table 12–7using the administration console. If External Oracle HTTP Servers are being used, then routes only required for IDMINTERNAL.mycompany.com. All other routing will take place on the Oracle HTTP Server.

Table 12–7 Routes and Conditions

Virtual Host	Route	Origin-Server Pool	Conditions	Cookie Name
iadadmin.mycompany.com	default	iadadmin-pool	N/A	
	oaam-admin-route	oaam-admin-pool	$uri =~ '/oaam_admin'	
igdadmin.mycompany.com	default	igdadmin-pool	NA	
	oim-admin-route	oim-pool	$uri =~ '/oim' or $uri =~ '/identity' or $uri =~ '/sysadmin' or $uri =~ '/xlWebApp' or $uri =~ '/Nexaweb'	oimjsessionid
sso.mycompany.com	default	origin-server-pool-1	N/A	OAM_JSESSIONID

Table 12–7 (Cont.) Routes and Conditions

Virtual Host	Route	Origin-Server Pool	Conditions	Cookie Name
	oaam-route	oaam-pool	$uri =~ '/oaam_server'	OAM_JSESSIONID
	oim-sso-route	oim-pool	$uri =~ '/identity' or $uri =~ '/xlWebApp' or $uri =~ '/HTTPClnt' or $uri =~ '/reqsvc'	oimjsessionid
idminternal.mycompany.com	default	oim-pool	N/A	oimjsessionid
	soa-idminternal-route	soa-pool	$uri =~ '/soa-infra' or $uri =~ '/sodcheck' or $uri =~ '/integration' or $uri =~ '/ucs'	oimjsessionid

To create virtual server routes:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button that is situated at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to configure routes, for example `sso.mycompany.com`.
4. In the navigation pane, expand **Virtual Servers**, expand the **sso.mycompany.com** virtual server, and select **Routes**.

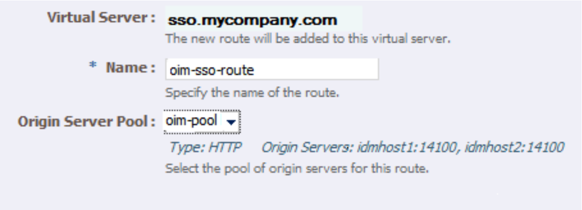
   The Routes page is displayed. It lists the routes that are currently defined for the virtual server.

   Creating a Route

   a. Click **New Route**.

      The New Route dialog box is displayed.

Figure 12–5 New Route Dialog Box



Virtual Server : sso.mycompany.com
The new route will be added to this virtual server.

* Name : oim-sso-route
Specify the name of the route.

Origin Server Pool : oim-pool
Type: HTTP   Origin Servers: idmhost1:14100, idmhost2:14100
Select the pool of origin servers for this route.

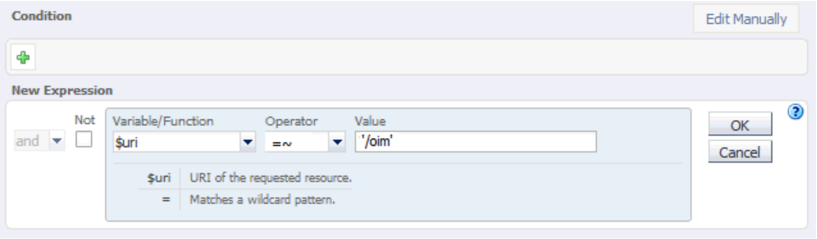
b. In the Step 1: Route Properties screen, in the **Name** field, enter `oim-sso-route`

c. In the Origin Server Pool drop-down select `oim-pool`, and click **Next**.

d. In the Step 2: Condition Information screen, select the **$uri** variable from the **Variable/Function** drop-down list. Select the Operator ('= ~ ' in your example). And enter the value in the **Value** field.

> **Note:** Joiner, such as `and` or `or`, cannot be used for the first expression in the sequence.

Figure 12–6 New Route Condition Expressions

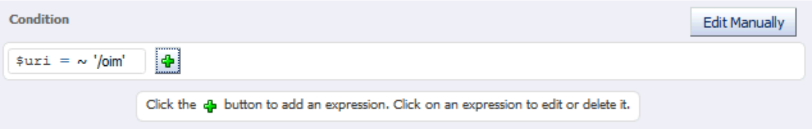


Variable/Function: $uri
Operator: =~
Value: '/oim'

$uri URI of the requested resource.
= Matches a wildcard pattern.

e. Click **OK** and click the **Plus** button to add the next expression.

Figure 12–7 New Route Condition Information

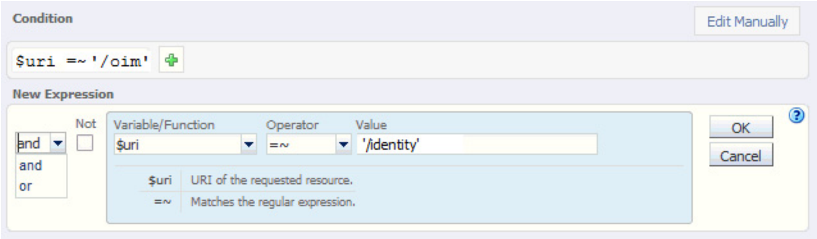


`$uri = ~ '/oim'`

Click the button to add an expression. Click on an expression to edit or delete it.

f. Select the **Variable/Function**, **Operator**, and **Value** and click **OK**.

Figure 12–8 New Route Condition Information



`$uri =~ '/oim'`

Joiner: and
Variable/Function: $uri
Operator: =~
Value: '/identity'

$uri URI of the requested resource.
=~ Matches the regular expression.

Note the joiner **'or'** can now be selected.

g. Perform steps **d** to **g** until you have added all the required values

You can also click the **Edit Manually** button to edit the expressions in a text field. Note that going into the manual mode, it is not possible to go back to the default edit mode. You must continue in the manual edit mode and save the condition.

5. Click **Next**, and then **Create Route**.

The route that you just created is displayed on the Routes page.

In addition, the **Deployment Pending** message is displayed at the top of the main pane. You can either deploy the updated configuration immediately by clicking

Deploy Changes, or you can do so later after making further changes as described in Section 12.11, "Deploying the Configuration and Testing the Virtual Server Addresses."

6. Update the cookie name of the newly created route and the default route:

   a. Click on the newly created route.

   b. Expand the **Advanced Settings**

   c. Set **Sticky Cookie** to the cookie name from table Table 12–7.

   d. Set the **Sticky URI Parameter** to the cookie name from Table 12–7.

   e. Repeat these steps for the values listed in Table 12–7.

   Click **Save**.

12.9 Enabling SSL Passthrough for sso.mycompany.com

In the enterprise deployment, Topology SSL is terminated at the hardware load balancer and passed through to Oracle Traffic Director using the HTTP protocol. If an external HTTP server is being used, this section is not applicable.

Oracle Traffic Director requires extra configuration steps to ensure that any application redirects occur correctly.

To ensure application redirects occur correctly:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":

2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations is displayed.

3. Select the configuration for which you want to configure routes, for example `sso.mycompany.com`.

4. In the Navigation Pane, expand **Virtual Servers** and select the virtual server **sso.mycompany.com**.

5. Click **Routes**.

   The defined routes appear.

6. Click a route, for example, **default-route**.

   The Route Properties screen appears.

7. Expand **Advanced Settings**.

8. In the **Route Properties** section, remove any content in the box labeled **Rewrite Headers**.

9. In the **Parameters Forwarded to Origin Servers** section, deselect the following:

   - SSL
   - Cipher
   - Key Size
   - Secret Key Size
   - SSL/TLS Session ID
   - Certificate

- User DN
- Issuer DN

Click **Save**.

10. Repeat for each route associated with the virtual server sso.mycompany.com.

12.10 Workaround for Issues caused by TMPWATCH cleanup

When OTD runs, it creates files in `/tmp`. The UNIX process `TMPWATCH`, which cleans up the temporary directory, can delete these files. This effects OTD's operation.

To avoid this issue, Oracle Traffic Director must be told to place its files in a location other than `/tmp`.

To do direct OTD to do this:

1. Create a directory called `tmp` in *OTD_ORACLE_INSTANCE*.

   For example:

   ```
   mkdir LOCAL_CONFIG/tmp
   ```

2. Log in to the OTD Administration Console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs."
3. Click **Advanced Settings** from the **Configuration** menu.
4. In the **General Configuration** settings, update the value of **Temporary Directory** to *LOCAL_CONFIG*`/tmp`.
5. Click **Save**.

12.11 Deploying the Configuration and Testing the Virtual Server Addresses

Deploy the configuration to create an instance of it on an administration node. When you deploy a configuration, the running instances are reconfigured to reflect the configuration changes.

Note: The topology documented in this guide requires the following virtual IP addresses:

- idstore.mycompany.com
- idminternal.mycompany.com
- iadadmin.mycompany.com

You can add idstore.mycompany.com and idminternal.mycompany.com host entries to resolve them with and internal IP address.

You can register iadadmin.mycompany.com and igdadmin.mycompany.com on the DNS.

Deploying a Configuration Using the Administration Console

To deploy a configuration by using the administration console, do the following:

1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the **IAM** configuration.
4. Click **Deploy**.

   A message is displayed confirming that the updated configuration was successfully deployed.
5. Click **Close**.

12.12 Creating a Failover Group for Virtual Hosts

When a request is sent to one of the virtual hosts `idstore.mycompany.com` and `idminternal.mycompany.com` it is directed to the IP address associated with the virtual host name. This IP address is enabled on one of the OTD instances. In the case of failure, IP address is moved to an OTD instance that is still available.

Each OTD instance maintains a heart beat with each other OTD instance. If that heartbeat fails then OTD moves active IP addresses on the downed instance to one of the named failover instances. You do this by creating an active-passive failover group for the IP address. This failover group lists a primary and a number of secondary instances.

The enterprise deployment on Exalogic uses the following four failover groups:

- A failover group for distributing internal LDAP requests among the OUD servers.
- A failover group for internal inter-app requests.
- Two failover groups to allow the external load balancer requests among Oracle Traffic Director servers. This failover group is optional, as the load balancer could point to the OTD instances directly. The benefit of using an Oracle Traffic Director failover group is that failures are detected and resolved faster using the failover group resulting in a reduced recovery time from failed servers.

The steps below show you how to create failover groups with the information in Table 12–8.

Table 12–8 Failover Group Details

Virtual Host	Router ID	Network Prefix	Primary Node	Primary Network Interface	Secondary Node	Secondary Network Interface
idstore.mycompany.com	50	19	Admin Node	bond0	WEBHOST2	bond0
idminternal.mycompany.com	51	19	WEBHOST2	bond0	Admin Node	bond0
webhost1vhn1.mycompany.com	53	19	Admin Node	bond1	WEBHOST2	bond1
webhost2vhn1.mycompany.com	52	19	WEBHOST2	bond1	Admin Node	bond1

Note: The failover groups for the external virtual IP addresses are optional since the load balancer fails over requests between the two Oracle Traffic Director instances. However, they will provide faster failure detection and failover than the typical load balancer monitors.

Note: The router ID is a unique number you assign to the routing. The number must be between 1 and 244.

The Network Prefix is the subnet mask in the CIDR format.

The primary node is the node where the Failover group is initially active.

The Primary Network Interface is the interface on the host where the failover group is bound.

The Secondary Node is the Node on which the failover group can be started if the Primary node is unavailable.

The Secondary Network interface is the Network Interface used on the Secondary node.

To create a failover group by using the administration console, do the following:

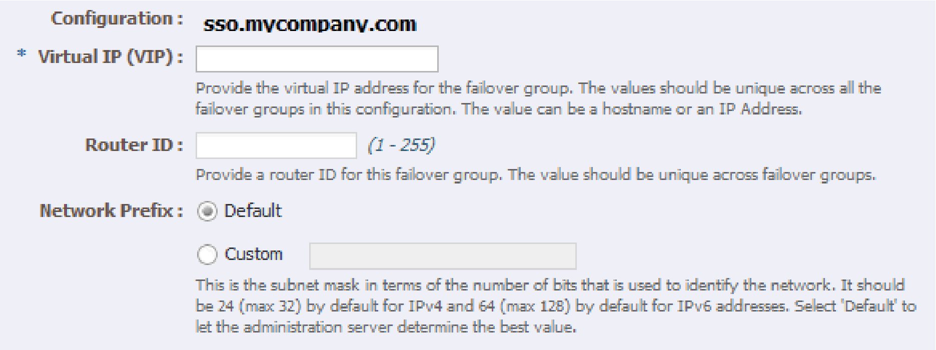
1. Log in to the OTD administration console using the URL specified in Section 20.2, "About Identity and Access Management Console URLs.":
2. Click the **Configurations** button at the upper left corner of the page.

   A list of the available configurations appears.
3. Select the configuration for which you want to create a failover group, for example `sso.mycompany.com`.
4. In the navigation pane, click **Failover Groups**.

   The Failover Groups page is displayed.
5. Click **New Failover Group**.

   The New Failover Group wizard is displayed.

Figure 12–9 New Failover Group Wizard



Configuration : **sso.mycompany.com**

* Virtual IP (VIP) :

Provide the virtual IP address for the failover group. The values should be unique across all the failover groups in this configuration. The value can be a hostname or an IP Address.

Router ID : *(1 - 255)*

Provide a router ID for this failover group. The value should be unique across failover groups.

Network Prefix : ● Default

○ Custom

This is the subnet mask in terms of the number of bits that is used to identify the network. It should be 24 (max 32) by default for IPv4 and 64 (max 128) by default for IPv6 addresses. Select 'Default' to let the administration server determine the best value.

6. In the **Virtual IP (VIP)** field, enter the virtual IP address associated with `idstore.mycompany.com` (192.168.50.2) and click **Next**.

To create the failover group for the `idminternal.mycompany.com` use the VIP associated with the `idminternal.mycompany.com` (192.168.50.1) as shown in Table 4–1.

7. In the Step 2: Failover Nodes Information screen, select the Primary and Backup nodes, (OTDADMIN, WEBHOST2), and click **Next**.

   The details of the failover group that you just created are displayed on the Failover Groups page.

   > **Note:** Generally it is sufficient to leave **Network Interface (NIC)** at the default value of `Auto Detect`. If you leave the default, Oracle Traffic Director (OTD) determines which network interface card to use based on the IP address of the failover group. If, however, this is not easily derivable, for example, if you have not used a standard CIDR associated with the IP address, you may have to manually tell OTD the network interface to which the failover group should be attached.
   >
   > For example, if your internal IP address is 192.168.1.1, and it is associated with `bond0`, and uses a valid net mask (CIDR), and your IP address of the failover group is 192.168.50.1, OTD knows to use network interface `bond0`. If, however, OTD cannot determine the appropriate interface, you are required to specify it in this field.
   >
   > Oracle Traffic Director validates the information before creating the failover group.

8. Click **Close** on the Results screen.

   The details of the failover group that you just created are displayed on the Failover Groups page.

   > **Note:** A message may be displayed indicating that the failover group could not be started in the involved nodes due to insufficient privileges. To resolve this, log in to each node as root and run the following command:
   >
   > ```
   > OTD_ORACLE_HOME/bin/tadm start-failover --instance-home=WEB_
   > INSTANCE_HOME/ --config=sso.mycompany.com
   > ```

12.13 Backing Up the Oracle Traffic Director Configuration

Back up the Oracle Traffic director configuration. For more information, see Section Section 20.5, "Performing Backups and Recoveries."

13 Creating a Deployment Profile

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

This chapter describes the following wizard screens:

- Section 13.1, "Welcome."
- Section 13.2, "IAM Installation Options."
- Section 13.3, "Specify Security Updates."
- Section 13.4, "Describe Response File."
- Section 13.5, "Select IAM Products."
- Section 13.6, "Select Topology."
- Section 13.7, "Select Installation and Configuration Locations."
- Section 13.8, "Configure Virtual Hosts."
- Section 13.9, "Set User Names and Passwords."
- Section 13.10, "Configure Oracle Unified Directory."
- Section 13.11, "Configure Oracle HTTP Server."
- Section 13.12, "Configure Oracle Identity Manager."
- Section 13.13, "Configure Oracle Identity Manager Database."
- Section 13.14, "Configure SOA."
- Section 13.15, "Configure Oracle Access Manager."
- Section 13.16, "Configure Oracle Access Manager Database."
- Section 13.17, "Configure HTTP/HTTPS Load Balancer."
- Section 13.18, "Summary."

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

Refer to the information you assembled in Section 11.1, "Assembling Information for Identity and Access Management Deployment." Variable names used in the screen descriptions in this chapter were introduced in that section.

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

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

Issue the command:

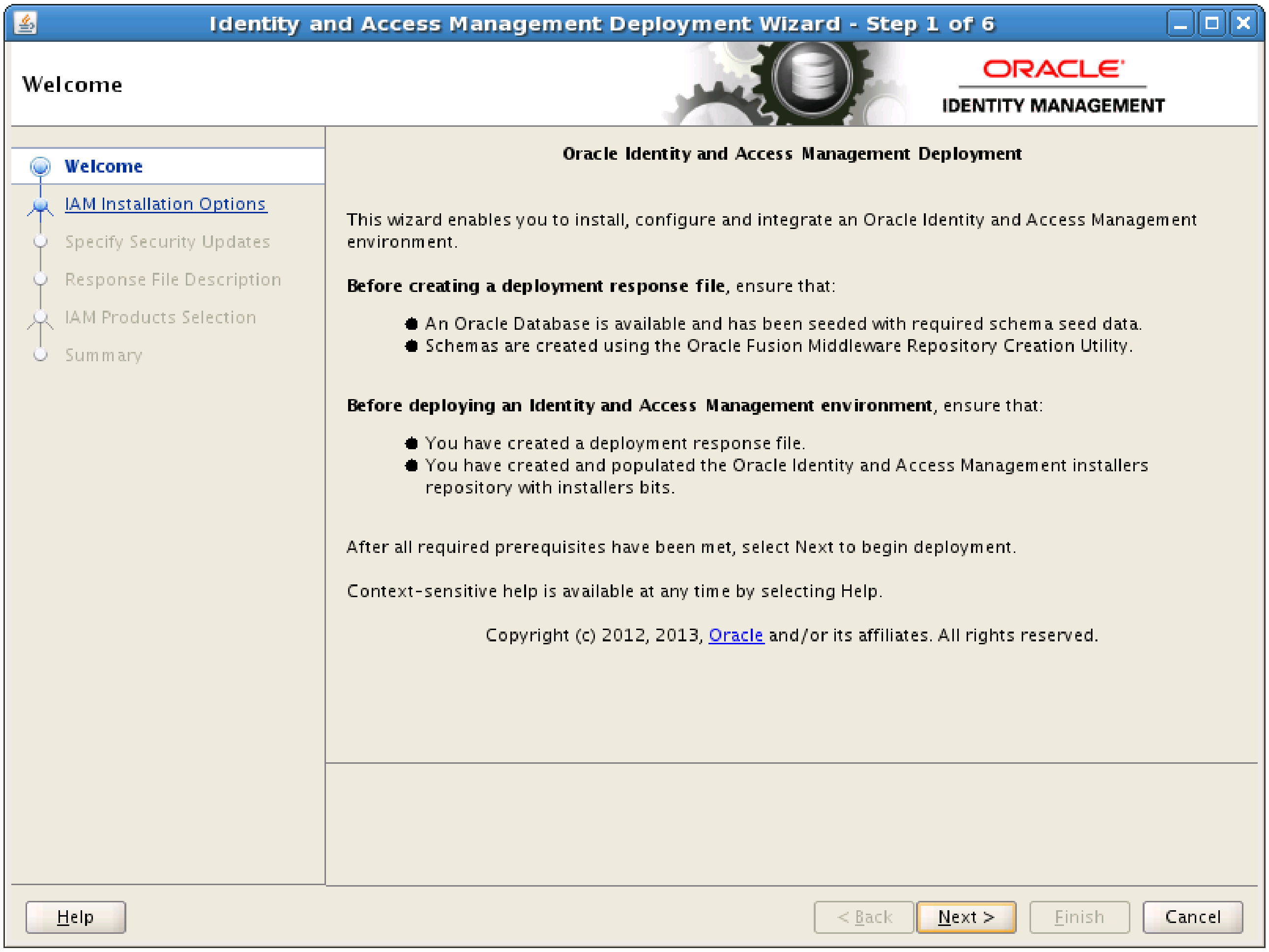
```
./iamDeploymentWizard.sh
```

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

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

13.1 Welcome

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



Oracle Identity and Access Management Deployment

This wizard enables you to install, configure and integrate an Oracle Identity and Access Management environment.

Before creating a deployment response file, ensure that:

- An Oracle Database is available and has been seeded with required schema seed data.
- Schemas are created using the Oracle Fusion Middleware Repository Creation Utility.

Before deploying an Identity and Access Management environment, ensure that:

- You have created a deployment response file.
- You have created and populated the Oracle Identity and Access Management installers repository with installers bits.

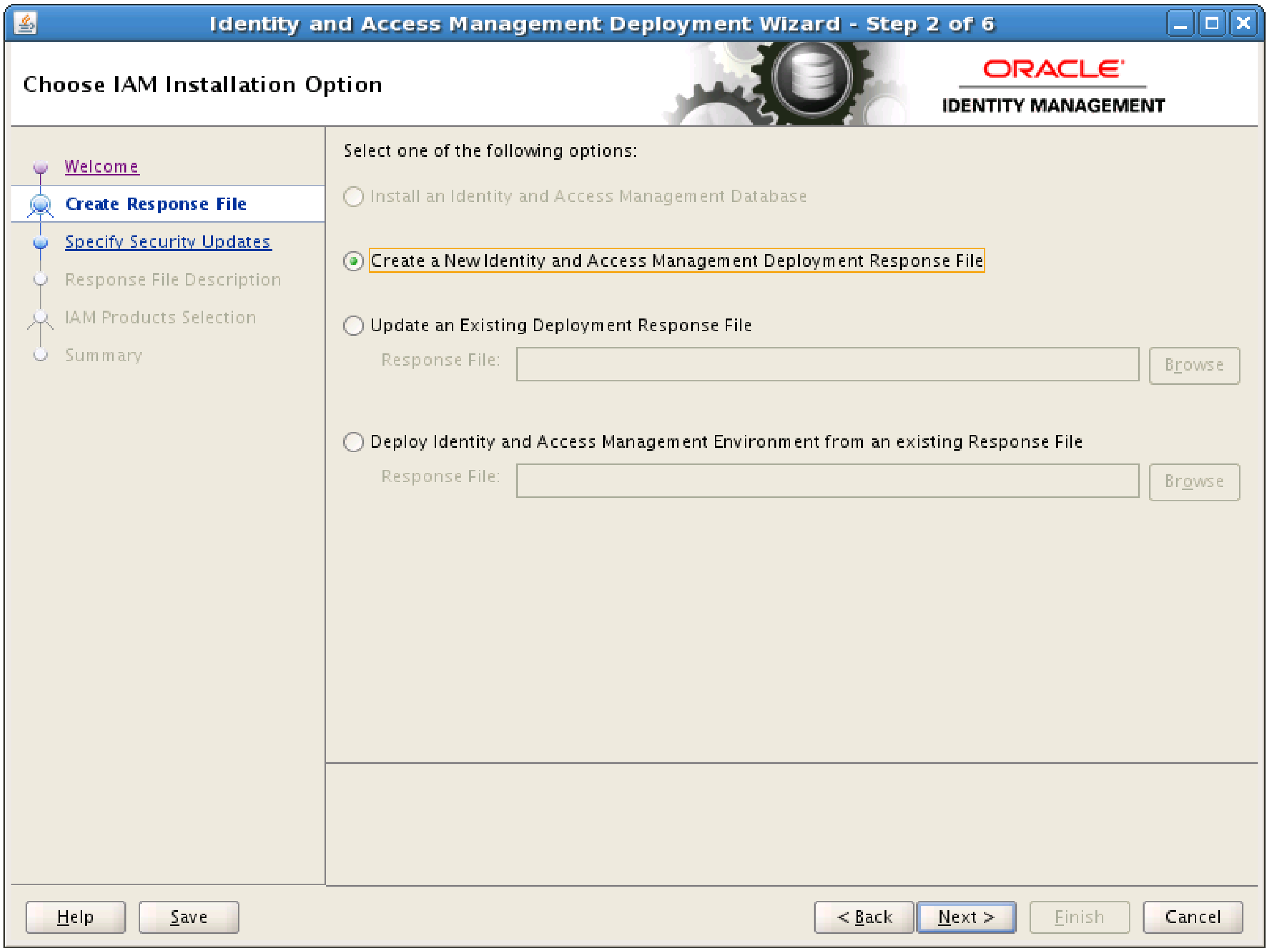
After all required prerequisites have been met, select Next to begin deployment.

Context-sensitive help is available at any time by selecting Help.

Copyright (c) 2012, 2013, Oracle and/or its affiliates. All rights reserved.

13.2 IAM Installation Options

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



Choose IAM Installation Option

Select one of the following options:

○ Install an Identity and Access Management Database

● Create a New Identity and Access Management Deployment Response File

○ Update an Existing Deployment Response File

Response File:

○ Deploy Identity and Access Management Environment from an existing Response File

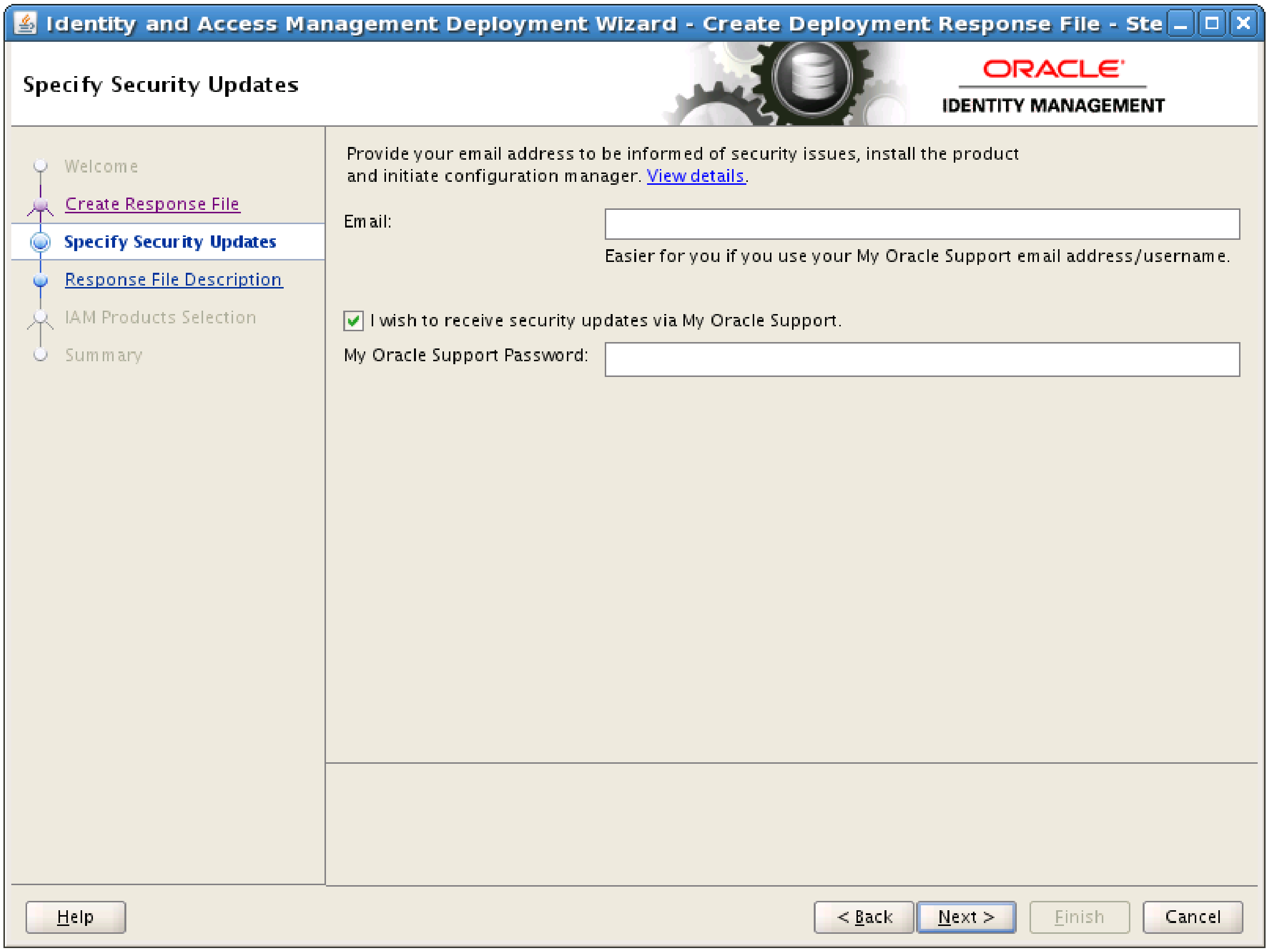
Response File:

13.3 Specify Security Updates

Use the Specify Security Updates screen to set up a notification preference for security-related updates and installation-related information from My Oracle Support. This information is optional.

- **Email**: Specify your email address to have updates sent by this method.
- **I wish to receive security updates via My Oracle Support**: Select this option to have updates sent directly to your My Oracle Support account. You must enter your My Oracle Support Password if you select this option.

Click **Next** to continue.



Provide your email address to be informed of security issues, install the product and initiate configuration manager. View details.

Email:

Easier for you if you use your My Oracle Support email address/username.

☑ I wish to receive security updates via My Oracle Support.

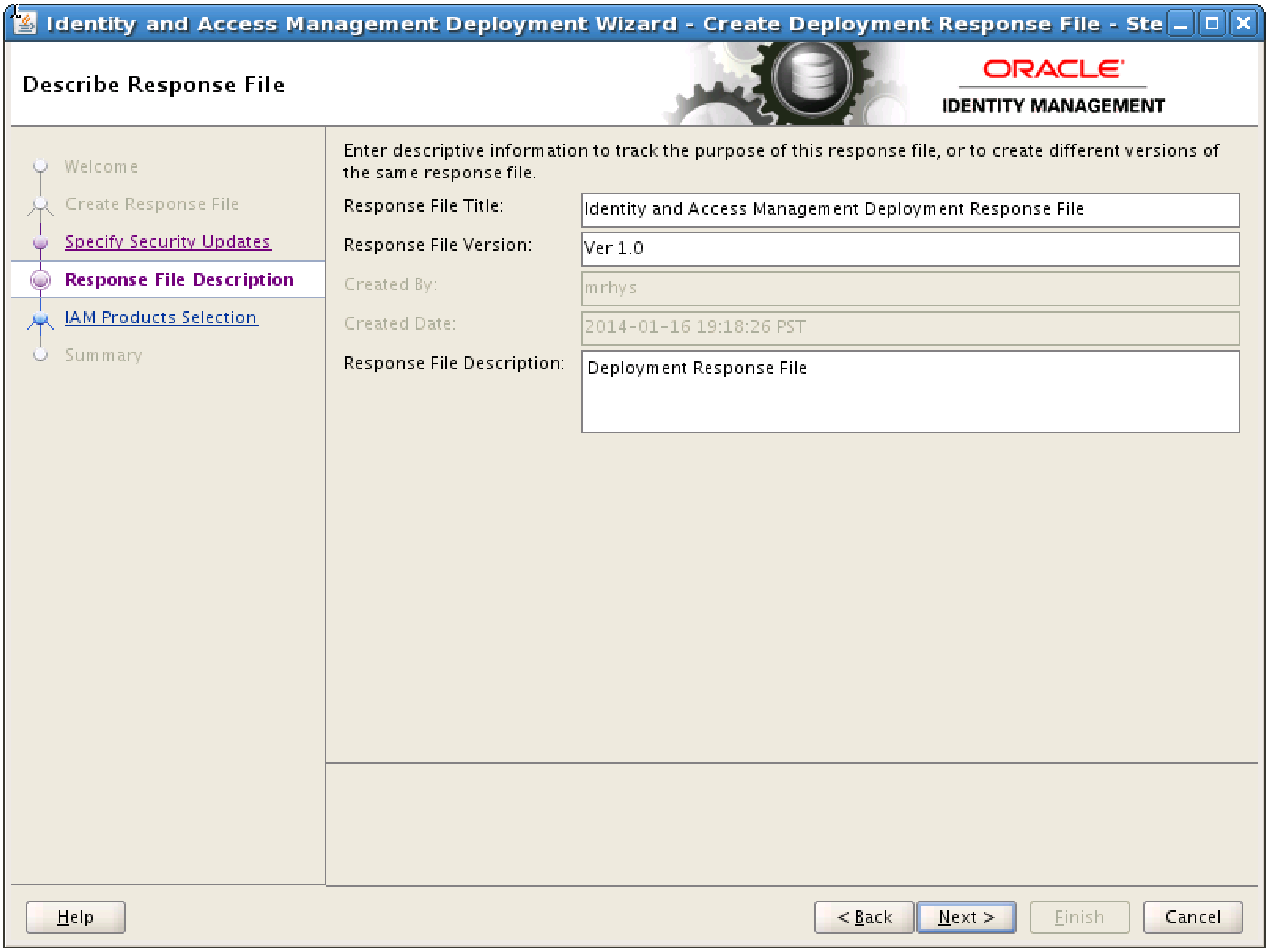
My Oracle Support Password:

13.4 Describe Response File

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

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

Click **Next**.



Identity and Access Management Deployment Wizard - Create Deployment Response File - Ste

Describe Response File

Enter descriptive information to track the purpose of this response file, or to create different versions of the same response file.

Response File Title: Identity and Access Management Deployment Response File

Response File Version: Ver 1.0

Created By: mrhys

Created Date: 2014-01-16 19:18:26 PST

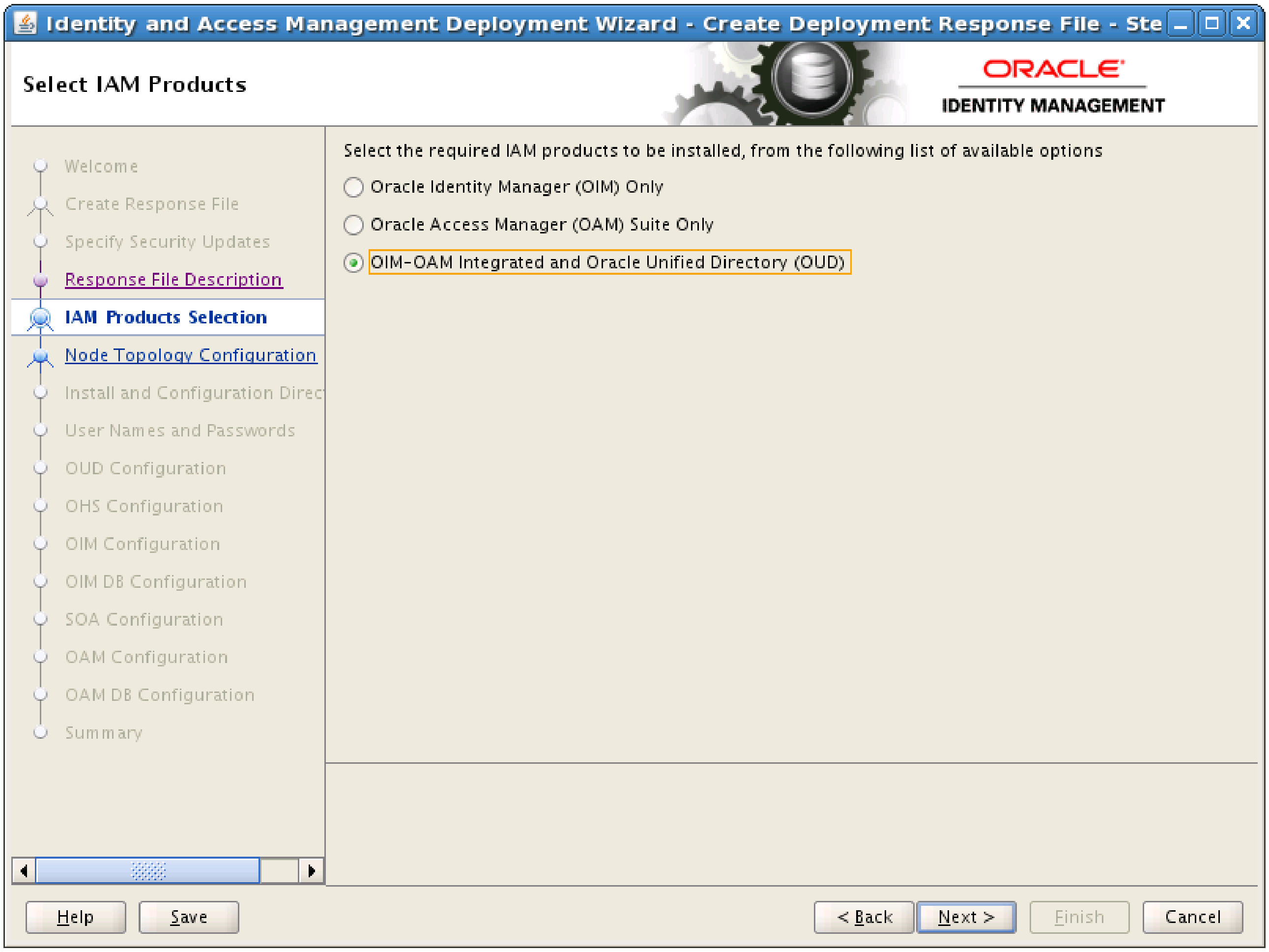
Response File Description: Deployment Response File

13.5 Select IAM Products

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

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

Click **Next**.



Select IAM Products

Select the required IAM products to be installed, from the following list of available options

○ Oracle Identity Manager (OIM) Only

○ Oracle Access Manager (OAM) Suite Only

● OIM-OAM Integrated and Oracle Unified Directory (OUD)

13.6 Select Topology

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

Note: All host names must be fully qualified.

Enter:

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

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

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

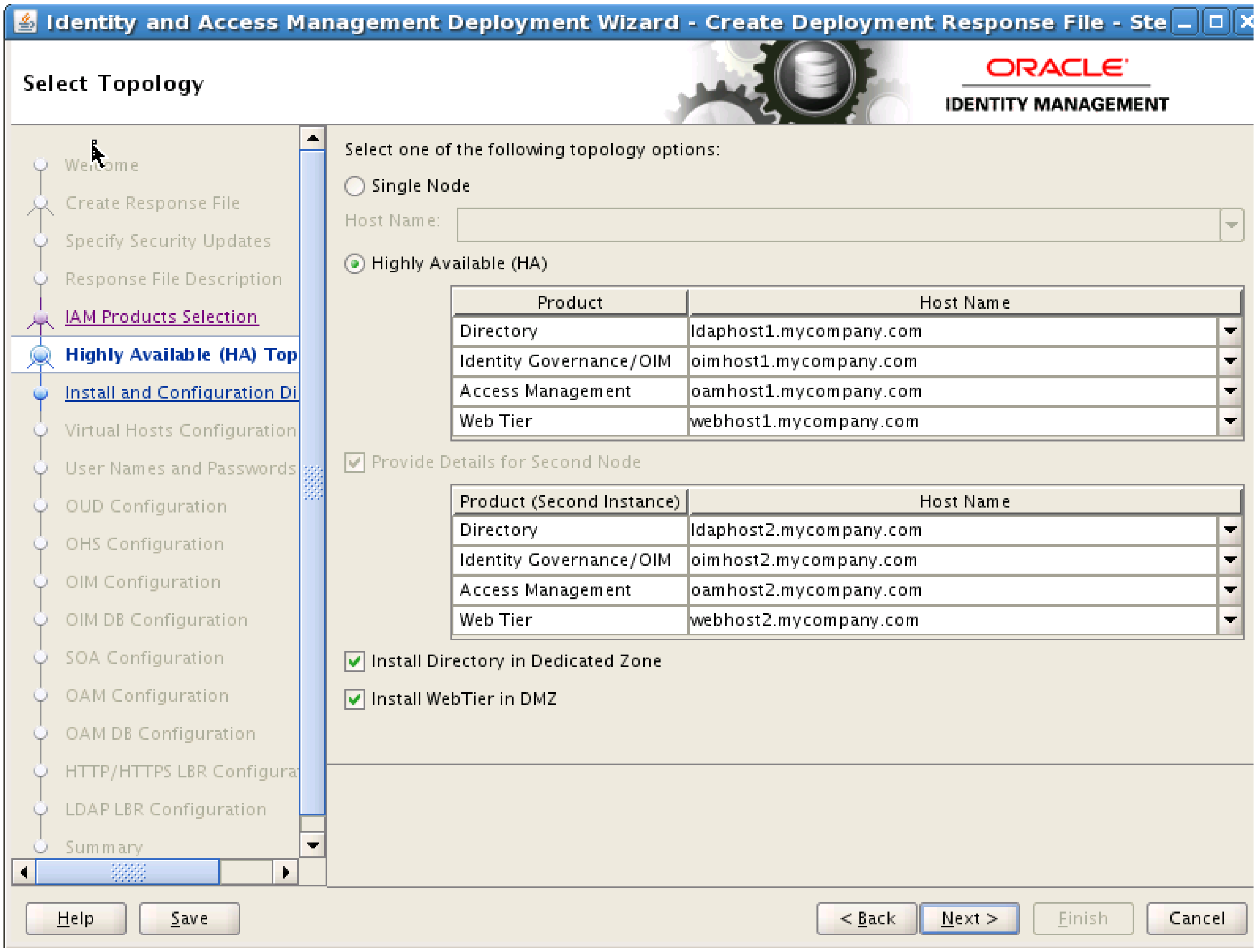
Note: If the topology has External Oracle HTTP Servers, enter OHSHOST1 and OHSHOST2 in the Web Tier prompts

---

Select **Install Directory in Dedicated Zone** if your directory servers are in a dedicated security zone and do not share the same *SW_ROOT* directory as the Identity Governance/Access Management Servers. If this option is selected, a separate *SW_ROOT* directory will be shared among the directory servers. See Chapter 7, "Preparing Storage for an Enterprise Deployment" for details.

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

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



Select one of the following topology options:

○ Single Node

Host Name:

● Highly Available (HA)

Product	Host Name
Directory	ldaphost1.mycompany.com
Identity Governance/OIM	oimhost1.mycompany.com
Access Management	oamhost1.mycompany.com
Web Tier	webhost1.mycompany.com

☑ Provide Details for Second Node

Product (Second Instance)	Host Name
Directory	ldaphost2.mycompany.com
Identity Governance/OIM	oimhost2.mycompany.com
Access Management	oamhost2.mycompany.com
Web Tier	webhost2.mycompany.com

☑ Install Directory in Dedicated Zone

☑ Install WebTier in DMZ

Notes:

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

Note: If you are creating a single instance high availability environment, do not select **Provide Details for Second Node**.

Click **Next**.

13.7 Select Installation and Configuration Locations

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

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

Note: As described in Section 9.10, "Mounting Shared Storage onto the Host," you should mount the *`LCM_HOME`* directory on every host for the duration of Identity and Access Management Deployment. If you have done this, select both of these **Mounted on ...** options.

If, however, you cannot mount the directory for the duration of provisioning, you can still perform deployment, but you must also perform some manual steps. See Section 14.4, "Deploying Identity and Access Management Without a Common LCM_HOME" for details.

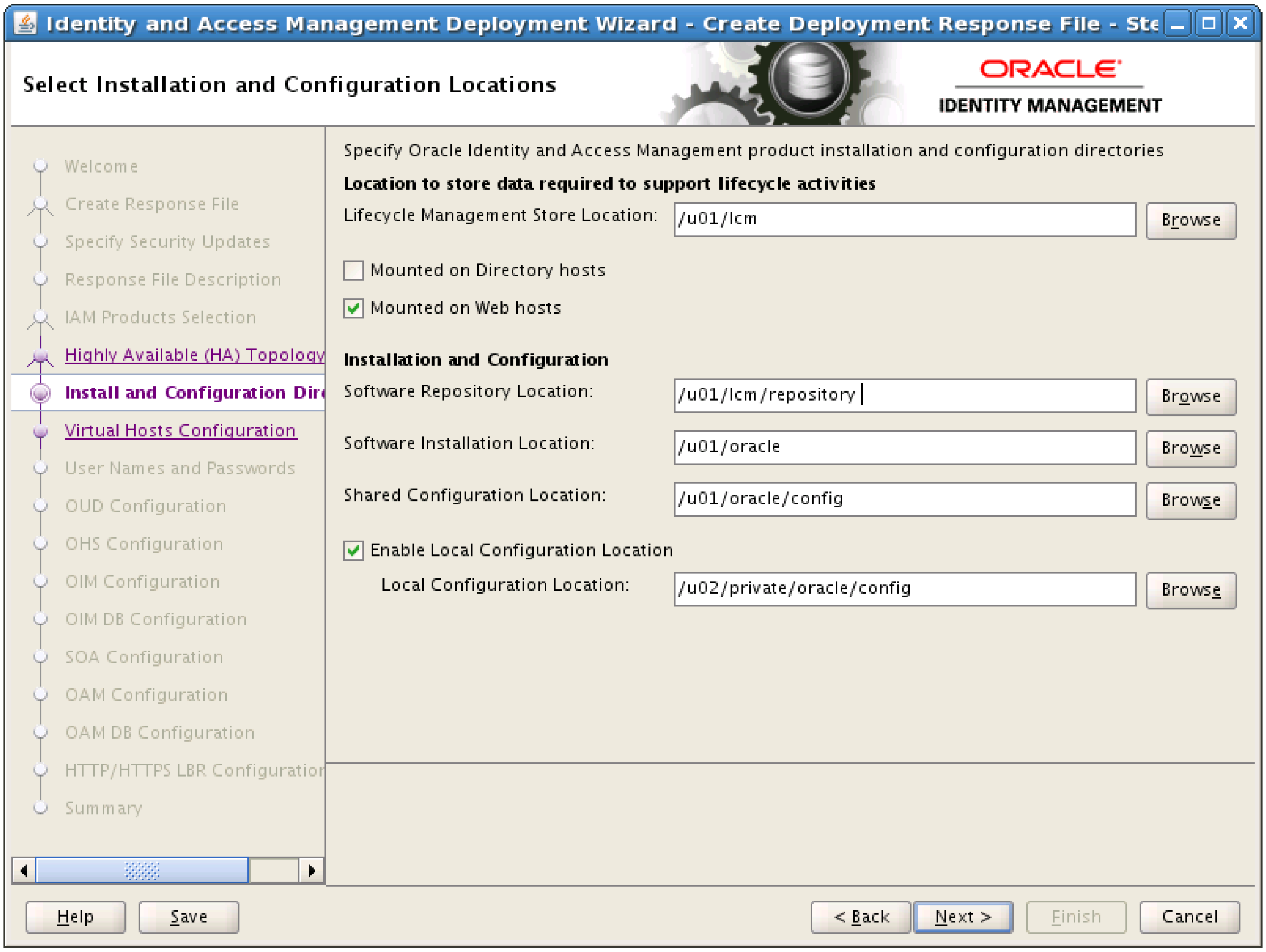
- **Software Repository Location**: This is the location of the Deployment repository, for example: `/u01/lcm/Repository` (*`REPOS_HOME`* in the worksheet).
- **Software Installation Location**: This is the location on shared storage under where you want the Middleware Home to be placed, for example: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

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

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

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

Click **Next**.



Specify Oracle Identity and Access Management product installation and configuration directories

Location to store data required to support lifecycle activities

Lifecycle Management Store Location: /u01/lcm

□ Mounted on Directory hosts

☑ Mounted on Web hosts

Installation and Configuration

Software Repository Location: /u01/lcm/repository

Software Installation Location: /u01/oracle

Shared Configuration Location: /u01/oracle/config

☑ Enable Local Configuration Location

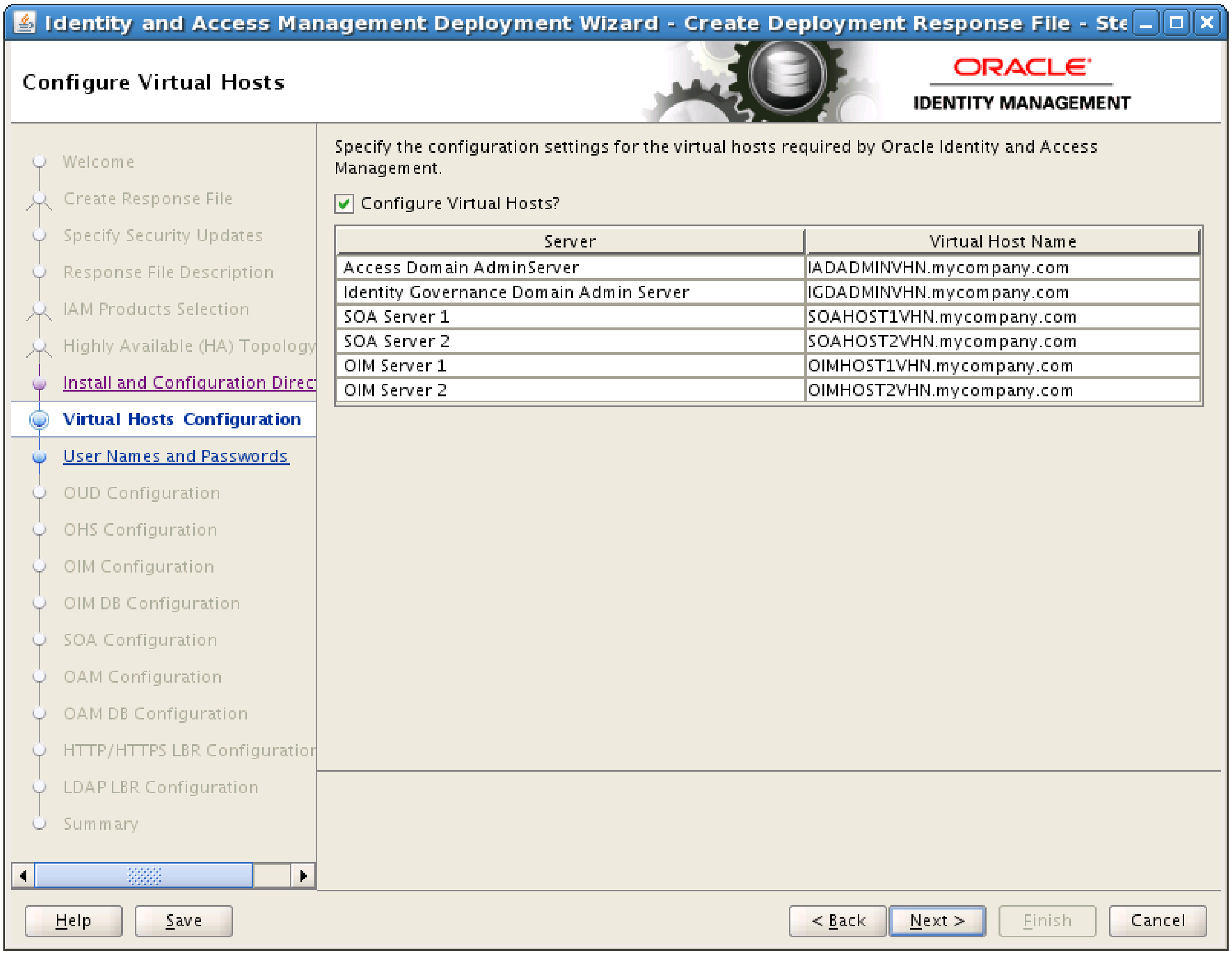
Local Configuration Location: /u02/private/oracle/config

13.8 Configure Virtual Hosts

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

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

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



Specify the configuration settings for the virtual hosts required by Oracle Identity and Access Management.

☑ Configure Virtual Hosts?

Server	Virtual Host Name
Access Domain AdminServer	IADADMINVHN.mycompany.com
Identity Governance Domain Admin Server	IGDADMINVHN.mycompany.com
SOA Server 1	SOAHOST1VHN.mycompany.com
SOA Server 2	SOAHOST2VHN.mycompany.com
OIM Server 1	OIMHOST1VHN.mycompany.com
OIM Server 2	OIMHOST2VHN.mycompany.com

Click **Next**.

13.9 Set User Names and Passwords

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

Enter Common IAM Password (*COMMON_IDM_PASSWORD*): This is the default password that will be used by all accounts unless overriden on an account by account basis.

Confirm Common IAM Password: Confirm the password.

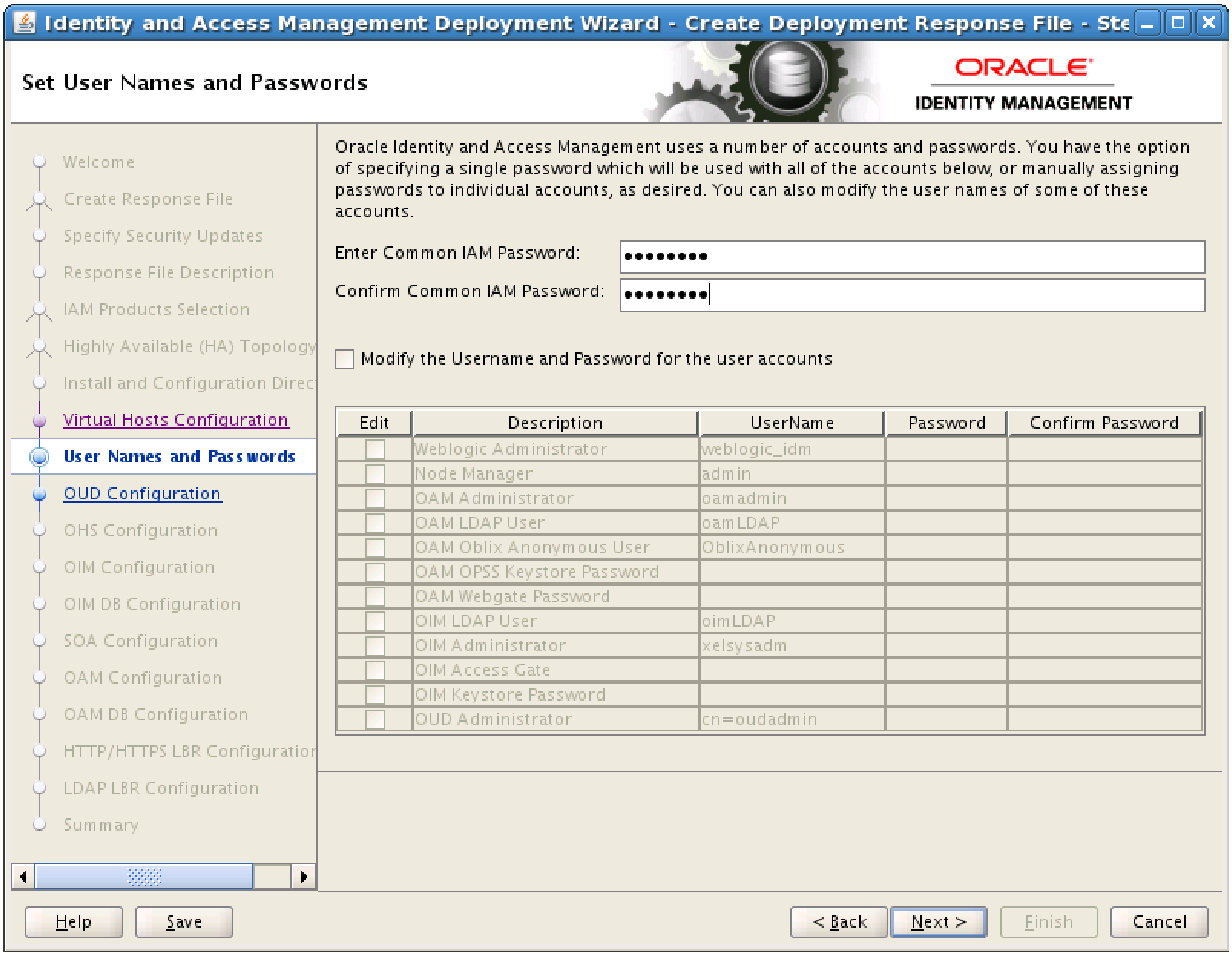
Note: For the purposes of this guide, assume that a Common IAM password is being used.

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

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

Override the Username and Password as desired.

Click **Next**.



Set User Names and Passwords

Oracle Identity and Access Management uses a number of accounts and passwords. You have the option of specifying a single password which will be used with all of the accounts below, or manually assigning passwords to individual accounts, as desired. You can also modify the user names of some of these accounts.

Enter Common IAM Password: ●●●●●●●●●

Confirm Common IAM Password: ●●●●●●●●●

□ Modify the Username and Password for the user accounts

Edit	Description	UserName	Password	Confirm Password
□	Weblogic Administrator	weblogic_idm		
□	Node Manager	admin		
□	OAM Administrator	oamadmin		
□	OAM LDAP User	oamLDAP		
□	OAM Oblix Anonymous User	OblixAnonymous		
□	OAM OPSS Keystore Password			
□	OAM Webgate Password			
□	OIM LDAP User	oimLDAP		
□	OIM Administrator	xelsysadm		
□	OIM Access Gate			
□	OIM Keystore Password			
□	OUD Administrator	cn=oudadmin		

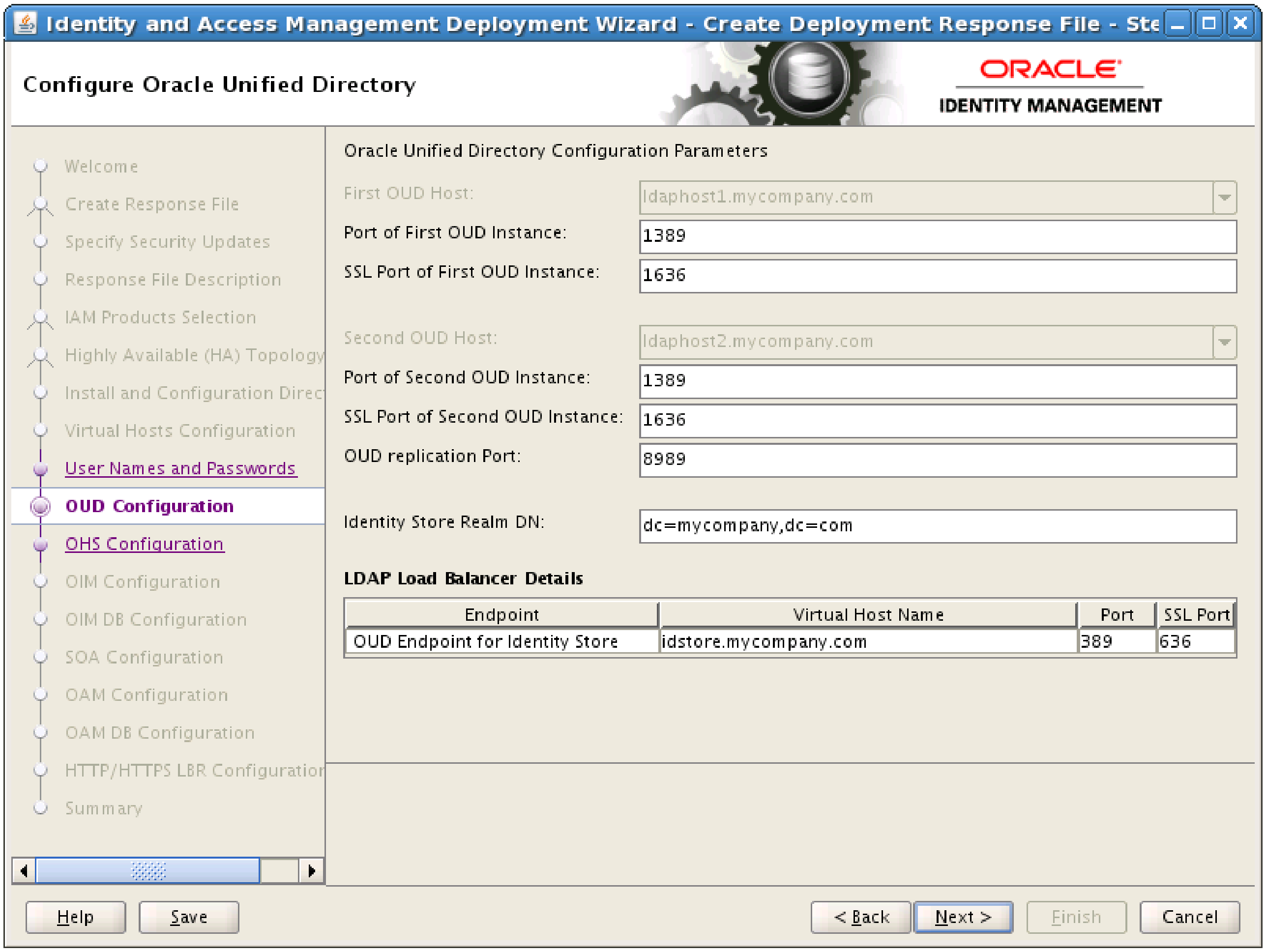
Click **Next**.

13.10 Configure Oracle Unified Directory

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

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

- **Endpoint**: The name of the endpoint, for example: `OUD Endpoint for ID Store`
- **Virtual Host Name**: The virtual host of the Identity store, for example: idstore.mycompany.com (*LDAP_IDSTORE_NAME*)
- **Port**: 1489 (*LDAP_LBR_PORT*)
- **SSL Port**: 1636 (*LDAP_LBR_SSL_PORT*)



Configure Oracle Unified Directory

Oracle Unified Directory Configuration Parameters

First OUD Host:	ldaphost1.mycompany.com
Port of First OUD Instance:	1389
SSL Port of First OUD Instance:	1636
Second OUD Host:	ldaphost2.mycompany.com
Port of Second OUD Instance:	1389
SSL Port of Second OUD Instance:	1636
OUD replication Port:	8989
Identity Store Realm DN:	dc=mycompany,dc=com

LDAP Load Balancer Details

Endpoint	Virtual Host Name	Port	SSL Port
OUD Endpoint for Identity Store	idstore.mycompany.com	389	636

Click **Next**.

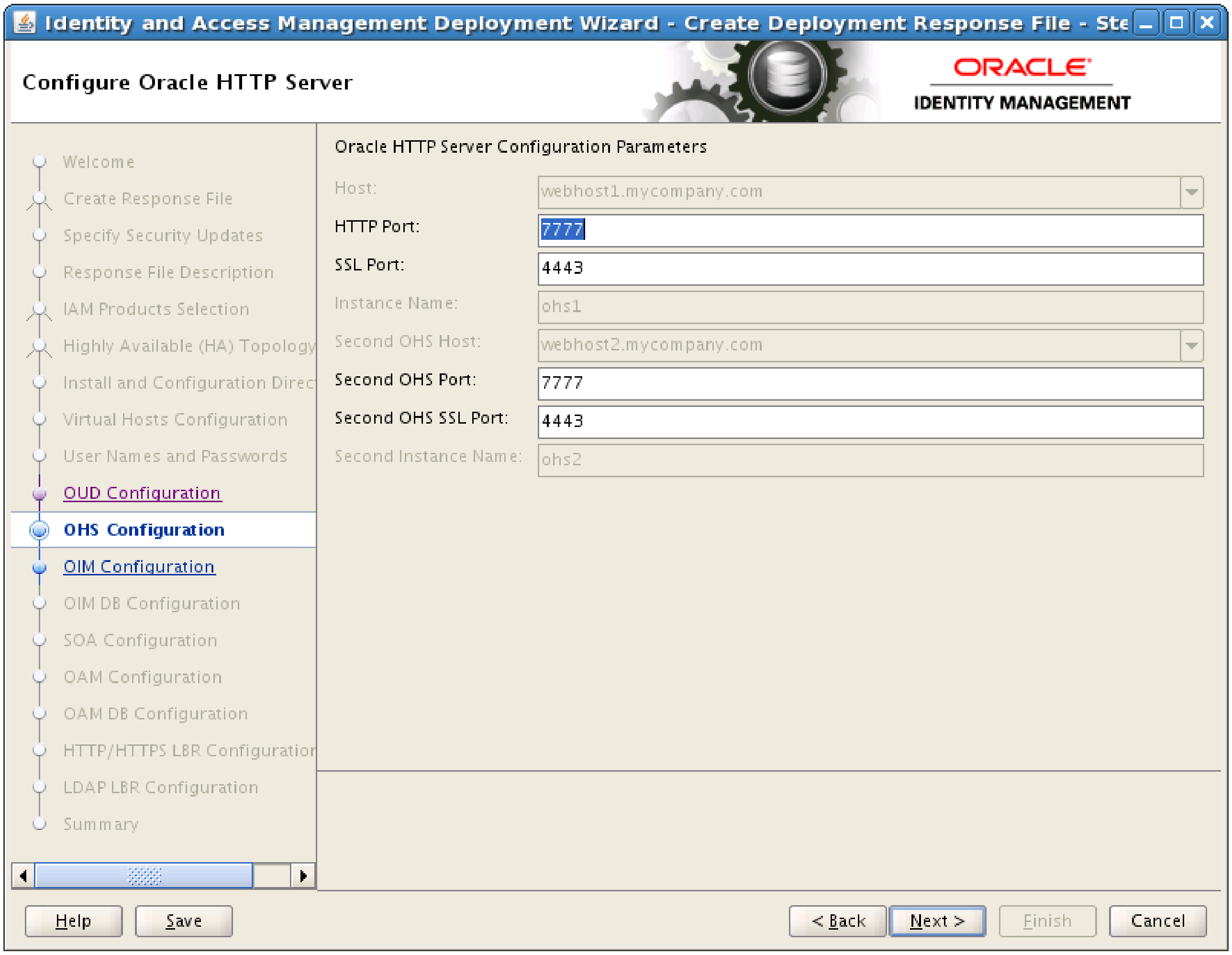
13.11 Configure Oracle HTTP Server

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

- **Port**: The port on which OHS listens for HTTP requests. For example: 7777 (*`WEB_HTTP_PORT`*)
- **SSL Port**: The port on which OHS listens for HTTPS requests. For example: 4443 (*`WEB_HTTPS_PORT`*)
- **Second OHS Port**: The port on which the second OHS listens for HTTP requests. For example: 7777 (*`WEB_HTTP_PORT`*)

- **Second OHS SSL Port**: The port on which the second OHS listens for HTTPS requests. For example: 4443 (*WEB_HTTPS_PORT*)

Click **Next**.



Configure Oracle HTTP Server

Oracle HTTP Server Configuration Parameters

Host:	webhost1.mycompany.com
HTTP Port:	7777
SSL Port:	4443
Instance Name:	ohs1
Second OHS Host:	webhost2.mycompany.com
Second OHS Port:	7777
Second OHS SSL Port:	4443
Second Instance Name:	ohs2

13.12 Configure Oracle Identity Manager

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

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

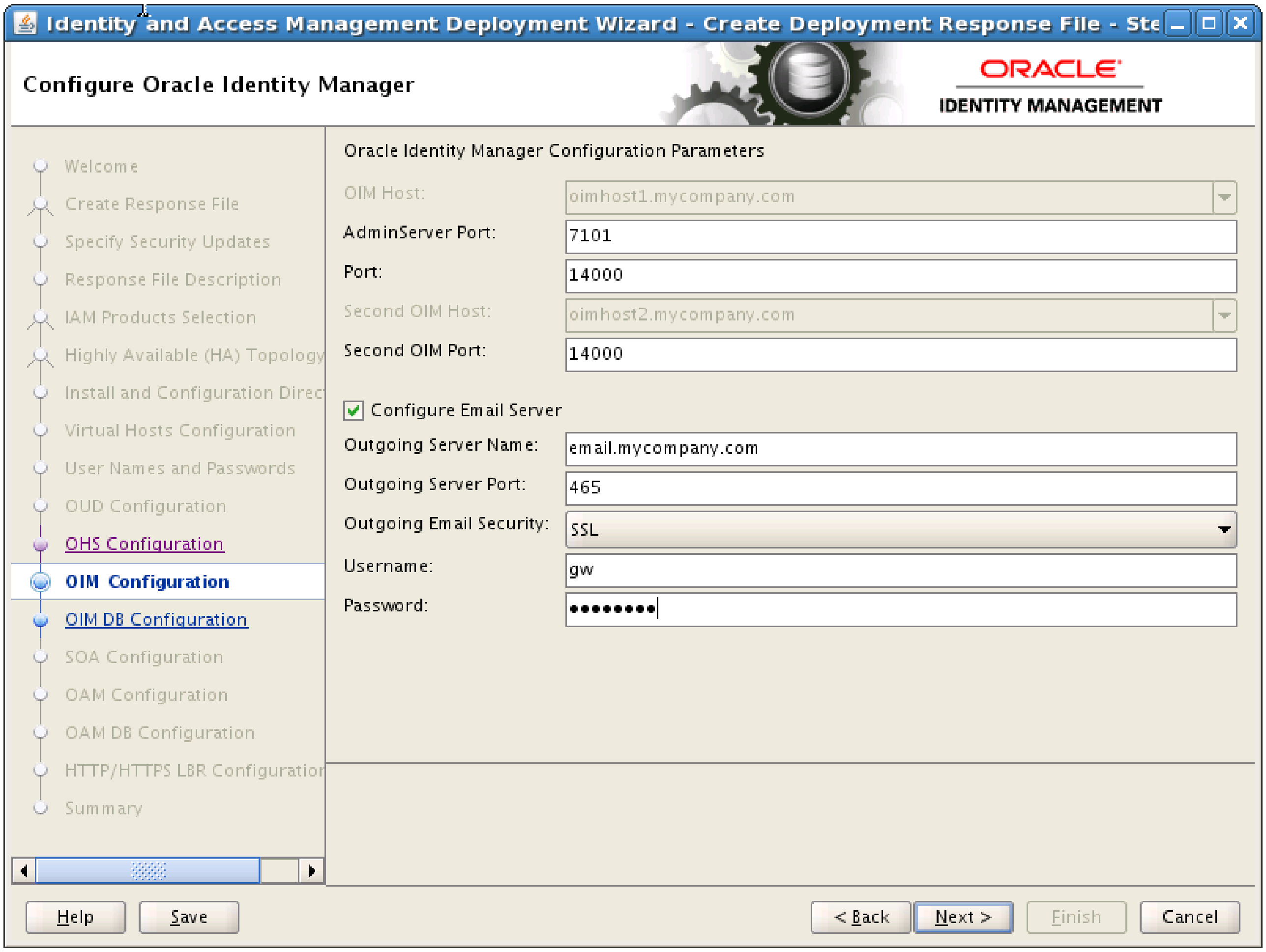
Port: The port number that the first OIM Managed Server will use, for example: 14000 (*OIM_PORT*)

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

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

- **Outgoing Server Name**: The name of your outgoing email server, for example: `EMAIL.mycompany.com` (*EMAIL_SERVER*)

- **Outgoing Server Port**: The port your email server uses, for example: 465 (*EMAIL_PORT*).
- **Outgoing Email Security**: Select None, SSL, or TLS (*EMAIL_PROTOCOL*)
- **Username**: The username (*EMAIL_USER*) you use to authenticate with the email server.
- **Password**: Password (*EMAIL_PASSWORD*) for the above user.



Configure Oracle Identity Manager

Oracle Identity Manager Configuration Parameters

OIM Host: oimhost1.mycompany.com

AdminServer Port: 7101

Port: 14000

Second OIM Host: oimhost2.mycompany.com

Second OIM Port: 14000

☑ Configure Email Server

Outgoing Server Name: email.mycompany.com

Outgoing Server Port: 465

Outgoing Email Security: SSL

Username: gw

Password: ●●●●●●●●

Click **Next**.

13.13 Configure Oracle Identity Manager Database

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

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

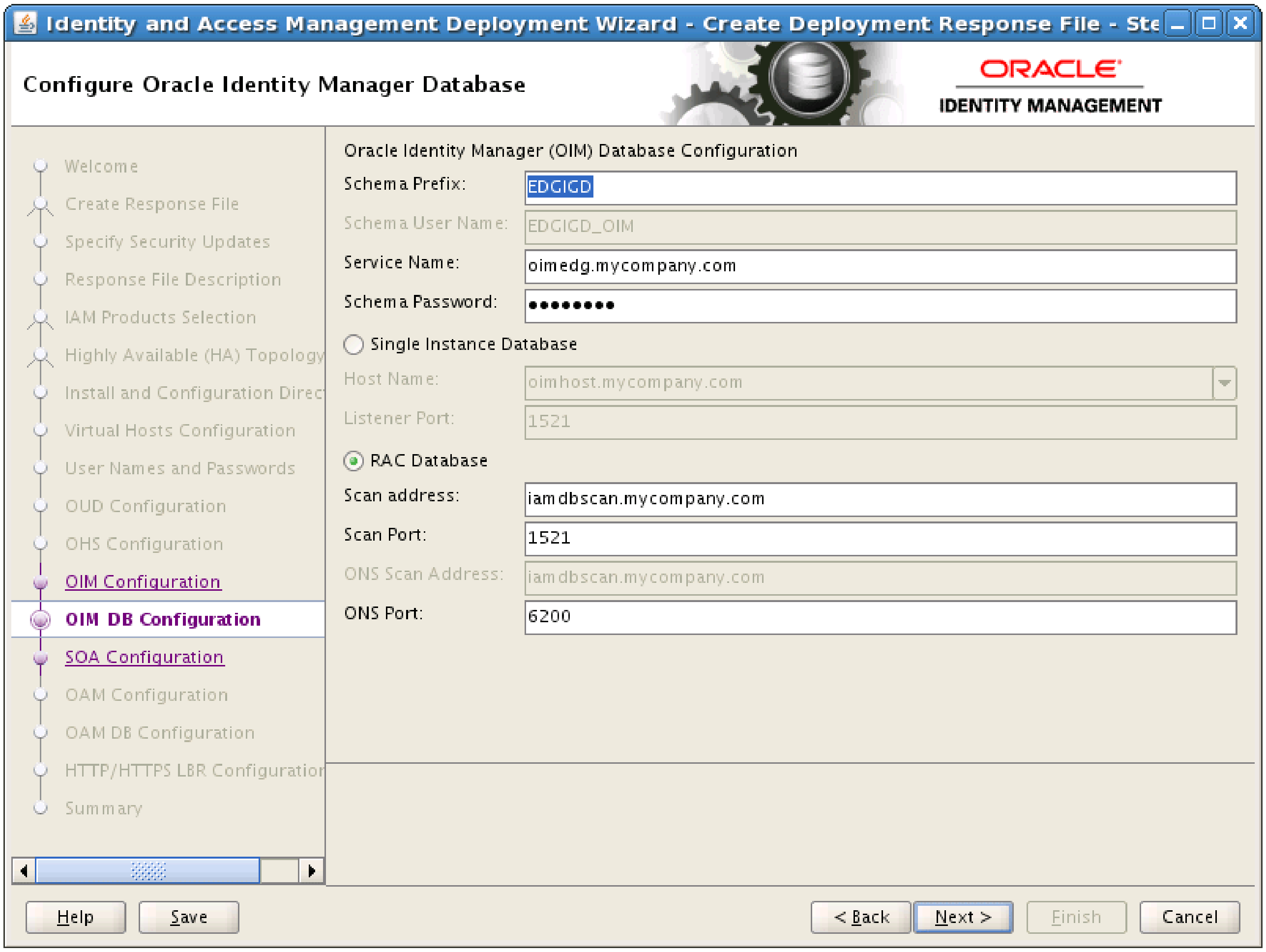
- **Scan Address**: Enter the Grid Infrastructure SCAN Address, for example: `IAMDBSCAN.mycompany.com` (*SCAN_ADDRESS*)

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

- **Scan Listener Port**: Enter the port used by the Grid Infrastructure Listener, for example: 1521 (*DB_LSNR_PORT*)
- **Scan port**: Determine the Scan (ONS) port by using the RAC `srvctl` command on the Oracle Database server, as shown in the following example:

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

Click **Next**.



Configure Oracle Identity Manager Database

Oracle Identity Manager (OIM) Database Configuration

Schema Prefix: EDGIGD

Schema User Name: EDGIGD_OIM

Service Name: oimedg.mycompany.com

Schema Password: ●●●●●●●●

○ Single Instance Database

Host Name: oimhost.mycompany.com

Listener Port: 1521

● RAC Database

Scan address: iamdbscan.mycompany.com

Scan Port: 1521

ONS Scan Address: iamdbscan.mycompany.com

ONS Port: 6200

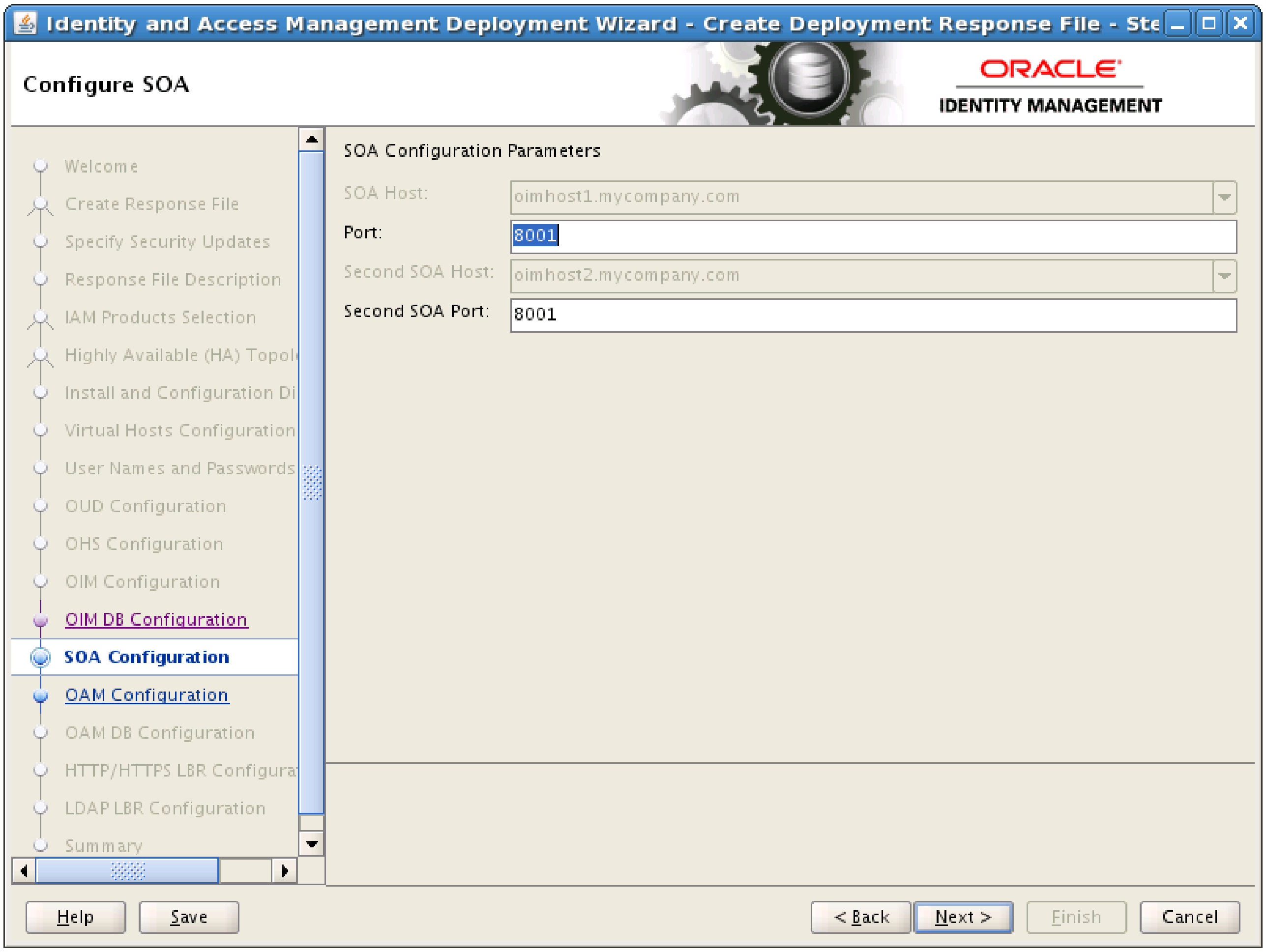
13.14 Configure SOA

Enter the following information:

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

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

Click **Next**



SOA Configuration Parameters

SOA Host: oimhost1.mycompany.com

Port: 8001

Second SOA Host: oimhost2.mycompany.com

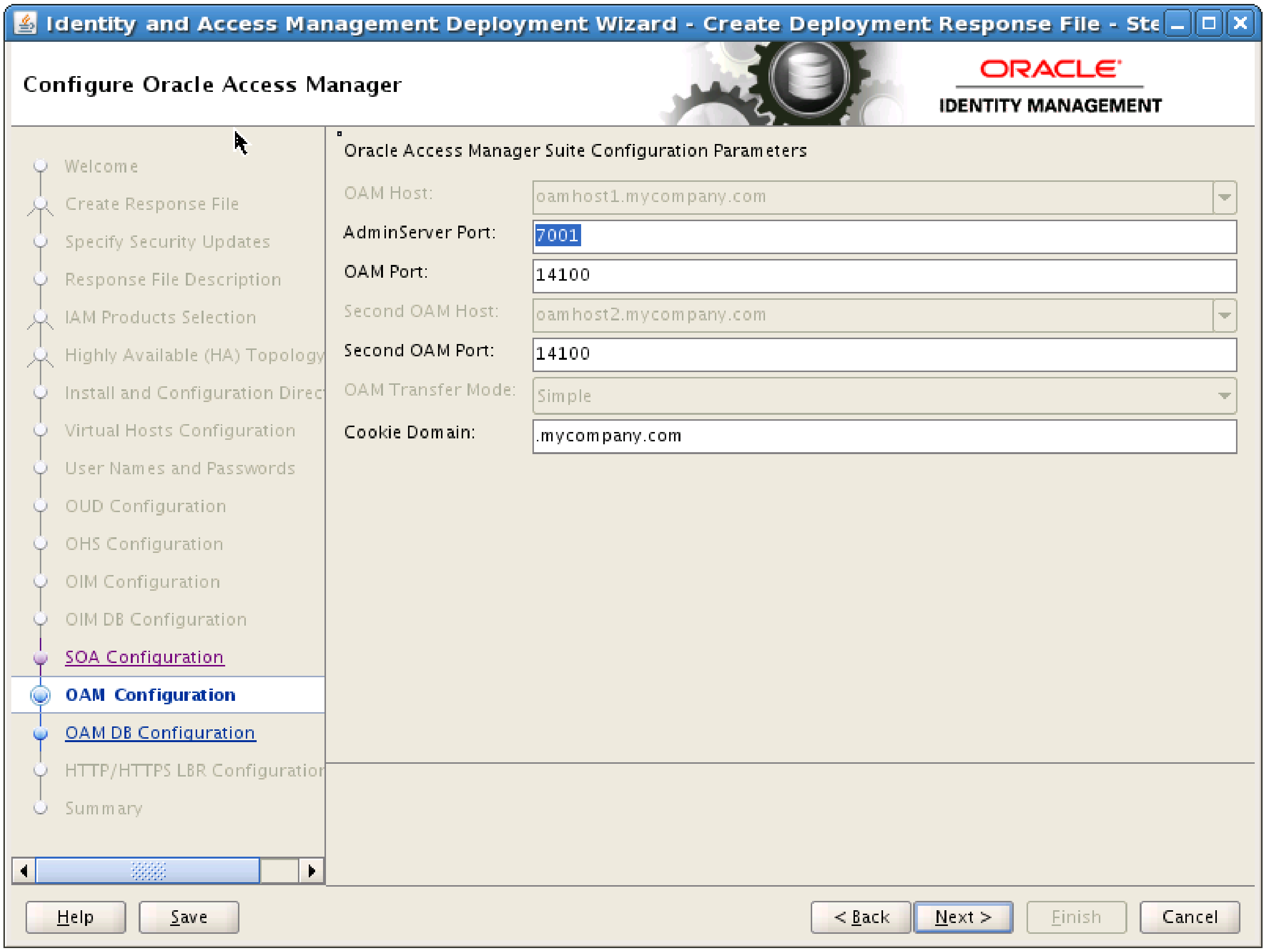
Second SOA Port: 8001

13.15 Configure Oracle Access Manager

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

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

Click **Next**.



Oracle Access Manager Suite Configuration Parameters

OAM Host: oamhost1.mycompany.com

AdminServer Port: 7001

OAM Port: 14100

Second OAM Host: oamhost2.mycompany.com

Second OAM Port: 14100

OAM Transfer Mode: Simple

Cookie Domain: .mycompany.com

13.16 Configure Oracle Access Manager Database

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

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

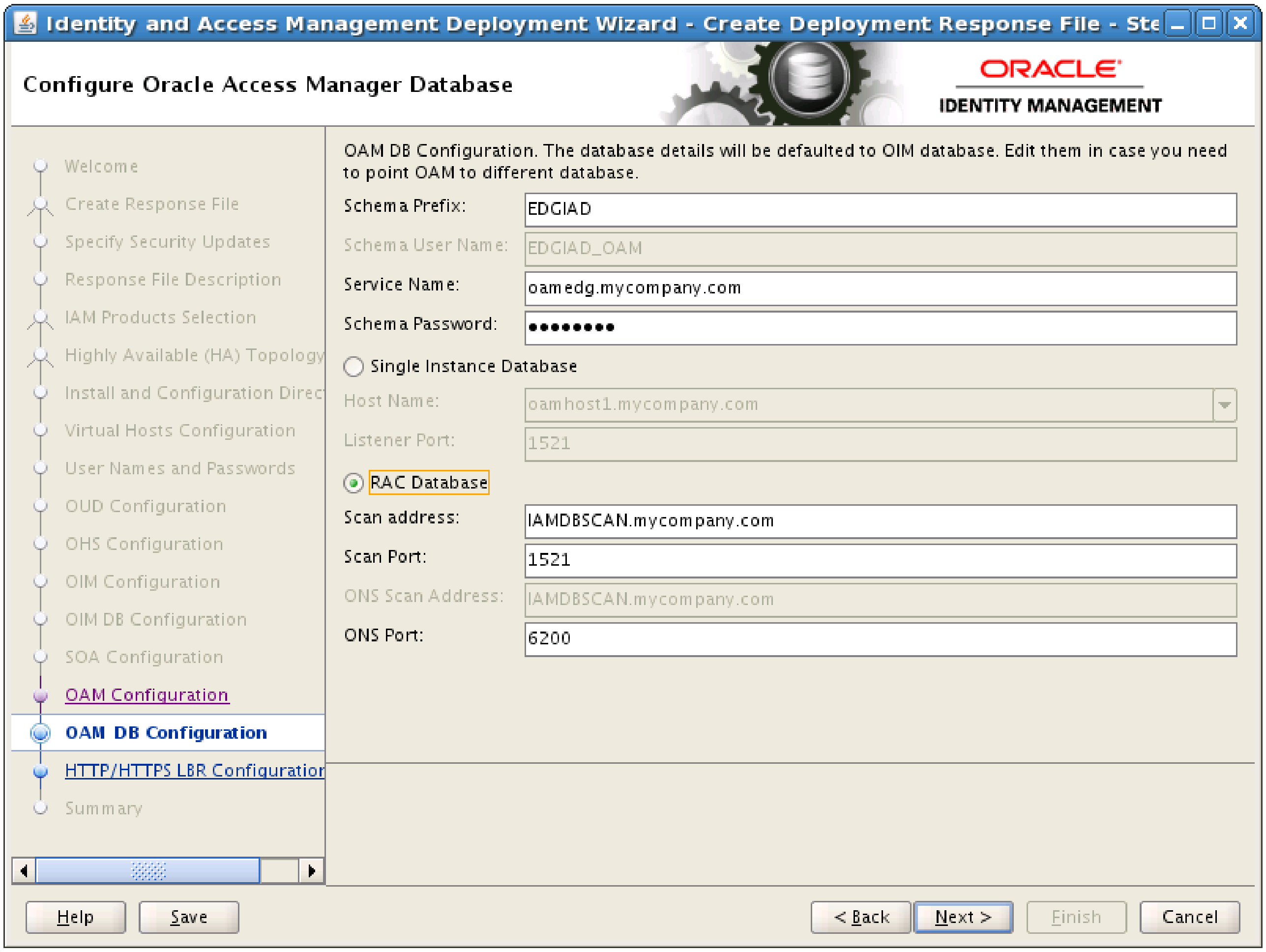
> **Note:** The default value for the Oracle Notification Server ONS) Scan Address, used by Gridlink, is the Database scan address.

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

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

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

Click **Next**.



Configure Oracle Access Manager Database

OAM DB Configuration. The database details will be defaulted to OIM database. Edit them in case you need to point OAM to different database.

Schema Prefix:	EDGIAD
Schema User Name:	EDGIAD_OAM
Service Name:	oamedg.mycompany.com
Schema Password:	••••••••
○ Single Instance Database	
Host Name:	oamhost1.mycompany.com
Listener Port:	1521
● RAC Database	
Scan address:	IAMDBSCAN.mycompany.com
Scan Port:	1521
ONS Scan Address:	IAMDBSCAN.mycompany.com
ONS Port:	6200

Click **Next**

13.17 Configure HTTP/HTTPS Load Balancer

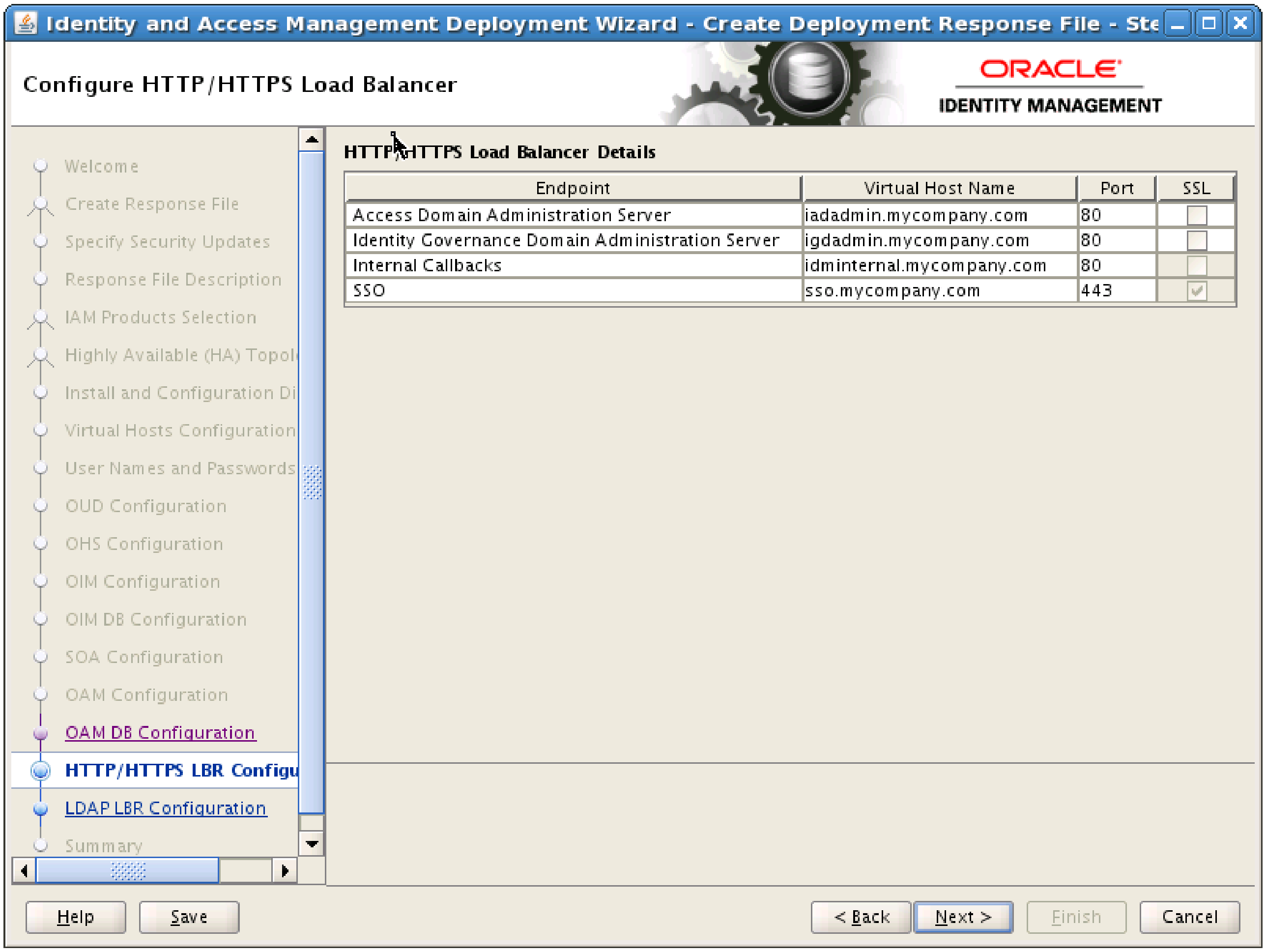
On the HTTP/HTTPS Load Balancer screen, enter details about your load balancer virtual hosts.

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

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

- **Internal Callbacks**: This is the internal call back virtual host and port (*IAM_INTERNAL_LBRVHN*), for example: `idminternal.mycompany.com`, Port `7777`
- **SSO**: This is the main application entry point (*IAM_LOGIN_LBRVHN*), for example: `sso.mycompany.com` Port `443`, always SSL.

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



Configure HTTP/HTTPS Load Balancer

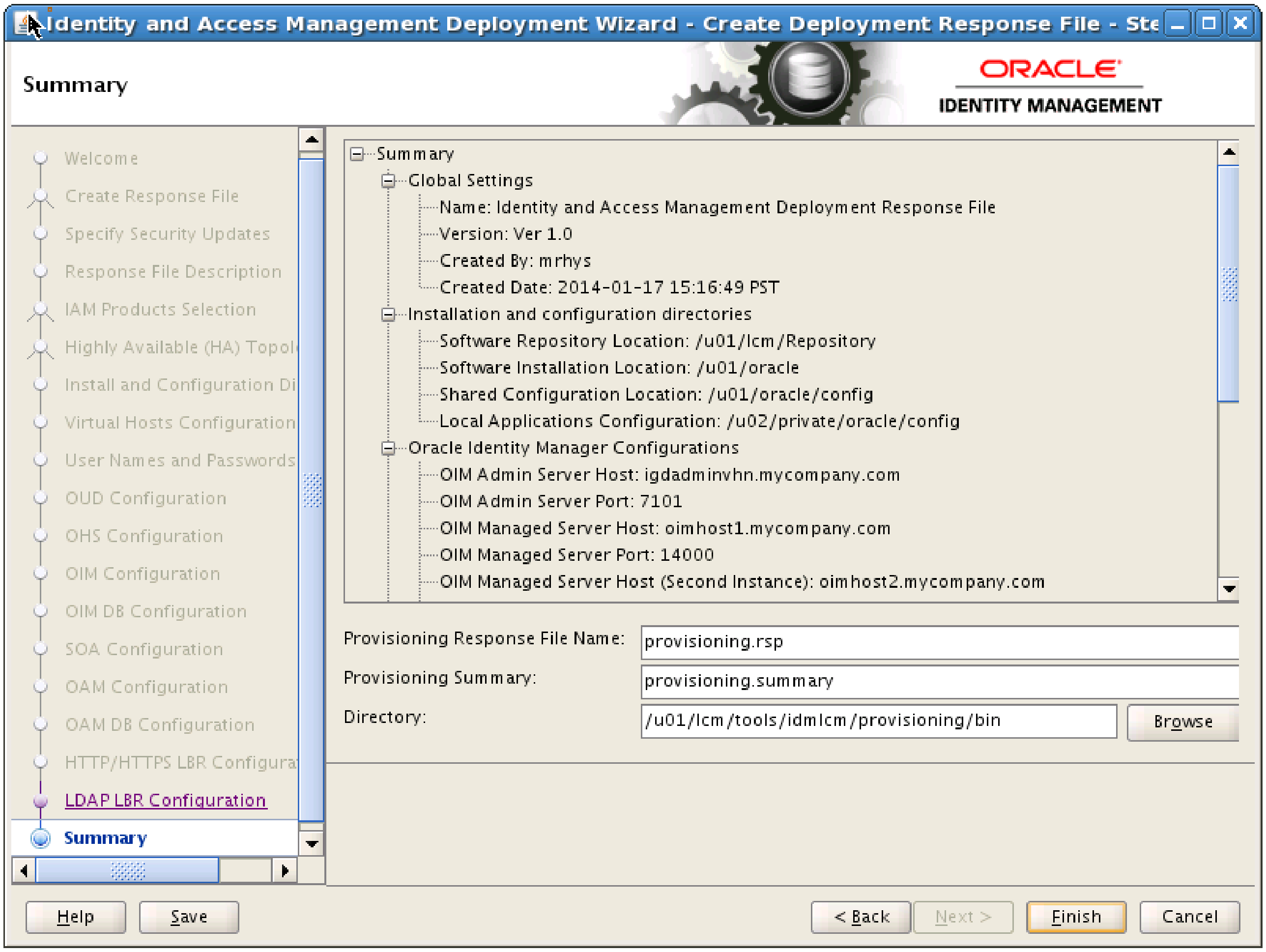
HTTP/HTTPS Load Balancer Details

Endpoint	Virtual Host Name	Port	SSL
Access Domain Administration Server	iadadmin.mycompany.com	80	□
Identity Governance Domain Administration Server	igdadmin.mycompany.com	80	□
Internal Callbacks	idminternal.mycompany.com	80	□
SSO	sso.mycompany.com	443	☑

13.18 Summary

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

The Identity and Access Management Deployment Wizard creates a deployment response file in the directory that you specify on the Summary screen. It also creates a folder named *responsefilename*`_data`, for example: `provisioning_data`. This folder contains the `cwallet.sso` file, which has encryption and decryption information. If you move or copy the deployment response file to another location, you must also move or copy the *responsefilename*`_data` folder containing the `cwallet.sso` file to the same location."



```
Summary
  Global Settings
    Name: Identity and Access Management Deployment Response File
    Version: Ver 1.0
    Created By: mrhys
    Created Date: 2014-01-17 15:16:49 PST
  Installation and configuration directories
    Software Repository Location: /u01/lcm/Repository
    Software Installation Location: /u01/oracle
    Shared Configuration Location: /u01/oracle/config
    Local Applications Configuration: /u02/private/oracle/config
  Oracle Identity Manager Configurations
    OIM Admin Server Host: igdadminvhn.mycompany.com
    OIM Admin Server Port: 7101
    OIM Managed Server Host: oimhost1.mycompany.com
    OIM Managed Server Port: 14000
    OIM Managed Server Host (Second Instance): oimhost2.mycompany.com
```

Provisioning Response File Name: provisioning.rsp

Provisioning Summary: provisioning.summary

Directory: /u01/lcm/tools/idmlcm/provisioning/bin

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

14 Deploying Identity and Access Management

This chapter describes how to deploy Identity and Access Management.

It contains the following sections:

- Section 14.1, "Introduction to the Deployment Process"
- Section 14.2, "Deployment Procedure"
- Section 14.3, "Check List"
- Section 14.4, "Deploying Identity and Access Management Without a Common LCM_HOME"

14.1 Introduction to the Deployment Process

This section introduces the deployment process.

14.1.1 Deployment Stages

There are eight stages to Deployment. These stages are:

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

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

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

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

14.1.2 Processing Order

You must process hosts in the following order:

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

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

Exalogic Physical Processing Order

1. IAMHOST1
2. IAMHOST2

Exalogic Virtual Processing Order

1. LDAPHOST1
2. LDAPHOST2
3. OIMHOST1
4. OIMHOST2
5. OAMHOST1
6. OAMHOST2
7. WEBHOST1

8. WEBHOST2

Exalogic Physical with External OHS Processing Order

1. IAMHOST1
2. IAMHOST2
3. OHSHOST1
4. OHSHOST2

   For information about the execution of automated LCM tool on the external OHS host, see Section 14.4, "Deploying Identity and Access Management Without a Common LCM_HOME."

14.2 Deployment Procedure

The following sections describe the procedure for performing Deployment.

- Section 14.2.1, "Running the Deployment Commands"
- Section 14.2.2, "Creating Backups"

14.2.1 Running the Deployment Commands

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

```
IDMLCM_HOME/provisioning/bin
```

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

Notes:

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

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

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

The commands you must run are:

```
runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target preverify

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target install

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target preconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target configure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
```

```
-target configure-secondary

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target postconfigure

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target startup

runIAMDeployment.sh -responseFile IDMLCM_HOME/provisioning/bin/provisioning.rsp
-target validate
```

14.2.2 Creating Backups

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

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

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

14.3 Check List

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

Physical

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

Deployment Stage	Host	Complete
Configure Secondary	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Post Configure	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Startup	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	
Validate	IAMHOST1	
	IAMHOST2	
	WEBHOST1	
	WEBHOST2	

Virtual

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

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

Deployment Stage	Host	Complete
Validate	LDAPHOST1	
	LDAPHOST2	
	OIMHOST1	
	OIMHOST2	
	OAMHOST1	
	OAMHOST2	
	WEBHOST1	
	WEBHOST2	

14.4 Deploying Identity and Access Management Without a Common LCM_HOME

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

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

1. Create a local version of the *LCM_HOME* directory, including the software repository.
2. Copy the Deployment Response File, *responsefilename*_data folder, and Summary created in Section 13.18, "Summary" to the same location on each of the hosts.
3. The deployment tool relies on the contents of the directories located under LCM_HOME/provisioning to determine what stages have run successfully. Therefore, after every command, copy the contents of this directory to every node before executing any runIAMDeployment.sh commands.

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

   LCM_HOME/internal is created after the install phase on the OAMHOSTs.
4. Before running preconfigure on OIMHOST1, copy *LCM_HOME*/keystores from LDAPHOST1 to OAMHOST1.
5. If *LCM_HOME* is not mounted on WEBHOST1 and WEBHOST2 (or OHSHOST1/OHSHOST2 in a topology with external Oracle HTTP Servers), before execution of the postconfigure phase on WEBHOST1, copy *LCM_HOME*/keystores/webgate_artifacts from OAMHOST1 to WEBHOST1 and WEBHOST2

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

15

Performing Post-Deployment Configuration

This chapter describes tasks you must perform after deployment.

It contains the following sections:

15.1 Enabling Oracle Traffic Director as a Web Server

This Section describes how to enable OTD as a web server. If you are using external Oracle HTTP servers, skip this section, as the Oracle HTTP Servers are providing the web server functionality.

15.1.1 Stop the OHS Servers

Stop the Oracle HTTP servers that the provisioning wizard created by executing the `opmnctl` command, which is located in the directory *`WEB_ORACLE_INSTANCE`*`/bin`, as follows:

```
opmnctl stopall
```

Perform this command on WEBHOST1 and WEBHOST2.

15.1.2 Stop the OHS Servers from Starting and Stopping Automatically

To stop the OHS servers starting and stopping automatically, proceed as follows:

1. Edit the file `serverInstancesInfo.txt` which is located in *`SHARED_CONFIG_DIR`*`/scripts`
2. Comment out the following lines by placing a **#** at the beginning of the line.

   ```
   webhost1 OHS /u02/private/oracle/config/instances/ohs1
   webhost2 OHS /u02/private/oracle/config/instances/ohs2
   ```

3. Repeat on each WEBHOST.

15.1.3 Reset the Oracle Traffic Director Listen Port

Now that provisioning is complete and the Oracle HTTP server is disabled, the OTD configuration must be updated with the OHS Listen Port. To do this perform the following steps:

1. Login to the OTD administration server using the URL:

   `https://OTDADMINVHN:8800`

2. Click **Configurations**, which is at the upper left corner of the page.

   A list of the available configurations is displayed.

3. Select the configuration which you want to amend, for example: **sso.mycompany.com**.
4. Expand **Listeners** in the Navigation pane.
5. Click **http-listener-1**
6. Set the port to *`WEB_HTTP_PORT`*, for example 7777.
7. Click **Save**.
8. Click **Deploy Changes**.

15.2 Post-Deployment Steps for OPSS

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

To upgrade the OPSS schema for EDGIAD (IAMAccessDomain) and EDGIGD (IAMGovernanceDomain):

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

   ```
   ./psa
   ```

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

   Click **Next**.

5. On the Schema Page, Enter:
   - **Database Type**: Oracle Database
   - **Connect String**: `IDMDB-SCAN`*`OAM`*`:`*`DB_LSNR_PORT`*`/`*`OAM_DB_SERVICENAME`* for example: `IAMDB-SCAN.mycompany.com:1521/oamedg.mycompany.com`
   - **DBA User Name**: `sys`
   - **DBA Password**: *`PASSWORD`*

   Click **Connect**.
6. Once you are connected successfully, enter the following:
   - **Schema User Name**: For example: `EDGIAD_OPSS`
   - **Password**: Password supplied when RCU was run.
7. On the Examine Page, verify that **Successful** is displayed and click **Next**.
8. On the Upgrade Summary Page verify that the information is correct and click **Upgrade**.
9. Once the upgrade is finished, click **Next**.
10. On the Upgrade Success page, click **Close**
11. Verify that the schema upgrade has been successful by checking the log files located in

    ```
    IAD_MW_HOME/oracle_common/upgrade/logs/psa/psatimestamp.log
    ```
12. Restart the domain as described in Section 20.1, "Starting and Stopping Components."
13. After upgrading the OPSS schema, run the following command:

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

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

15.3 Post-Deployment Steps for Oracle Unified Directory

This section describes post-deployment steps for Oracle Unified Directory.

This section contains the following topics:

- Section 15.3.1, "Update Oracle Unified Directory Change Log Access"
- Section 15.3.2, "Update Oracle Unified Directory ACIs for LDAP Synchronization"

15.3.1 Update Oracle Unified Directory Change Log Access

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

To grant access to the change log:

1. Create a file containing the `oudadmin` password.

   You can give this file any name, but for this example, name the file `mypasswordfile`. You can remove it after running the commands in this section.
2. Add the following new ACI:

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

For example:

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

15.3.2 Update Oracle Unified Directory ACIs for LDAP Synchronization

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

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

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

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

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

   Change:

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

   To:

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

2. Restart the Oracle Unified Directory server as described in Section 20.1, "Starting and Stopping Components."

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

```
java.lang.Exception: The request control with Object Identifier (OID)
"1.3.6.1.4.1.26027.1.5.4" cannot be used due to insufficient access rights
```

To avoid this error, add the following ACI:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\"1.3.6.1.4.1.26027.1.5.4\")(version 3.0; acl
\"OIMAdministrators control access\"; allow(read)
groupdn=\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
 --hostname LDAP_HOST \
 --port LDAP_ADMIN_PORT \
 --trustAll \
 --bindDN cn=oudadmin \
 --bindPasswordFile passwordfile \
 --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\"1.3.6.1.4.1.26027.1.5.4\")(version 3.0; acl
\"OIMAdministrators control access\"; allow(read)
groupdn=\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
 --hostname IDMHOST1.mycompany.com \
 --port 4444 \
 --trustAll \
 --bindDN cn=oudadmin \
 --bindPasswordFile mypasswordfile \
 --no-prompt
```

Restart the OUD server for the changes to take affect.

15.4 Post-Deployment Steps for Oracle Identity Manager

Perform the following post-deployment steps.

- Section 15.4.1, "Post Deployment Steps to Address Known Issue"
- Section 15.4.2, "Forcing OIM to use IPoIB for Multicast Operations"
- Section 15.4.3, "Workaround for Known Issue"
- Section 15.4.4, "Configuring Oracle Identity Manager Servers to Listen on EoIB"

15.4.1 Post Deployment Steps to Address Known Issue

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

1. Login to the WebLogic console for the domain using at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Lock and Edit**.
3. Navigate to **Environment > Servers**.

4. Click on a server name, for example: **wls_oam1**.
5. Click on the **SSL** tab.
6. Expand the **Advanced Options** and change **Hostname Verification** to **BEA Host Name Verifier**.
7. Click **Save**.
8. Repeat for each server in the domain.
9. Click **Activate Changes**.
10. Restart the domain.
11. Repeat for the second domain.

15.4.2 Forcing OIM to use IPoIB for Multicast Operations

As a workaround for a known issue in the Identity and Access Management Deployment tools, add an Oracle Identity Manager property.

To add the OIM property:

1. Log in to the WebLogic Console in the IAMGovernanceDomain. (The Console URLs are provided in Section 20.2, "About Identity and Access Management Console URLs.")
2. Navigate to **Environment -> Servers**.
3. Click **Lock and Edit**.
4. Click on the server **WLS_OIM1**.
5. Click on the **Server Start** subtab.
6. Add the following to the **Arguments** field:

   ```
   -Dmulticast.bind.address=oimhost1.mycompany.com
   ```

7. Click **Save**.
8. Repeat Steps 4-7 for the managed server **WLS_OIM2**.
9. Click **Activate Changes**.

> **Note:** Instead of using `oimhost1`, use the IPoIB name for the host on which the managed server runs. For example, `oimhost2` would be used for `oimhost2` in a virtual deployment and `iamhost1/2` would be used in a physical Exalogic deployments.

15.4.3 Workaround for Known Issue

As a workaround for a known issue in the Identity and Access Management Deployment tools, add an Oracle Identity Manager property.

To add the OIM property:

1. Log in to the WebLogic Console in the IAMGovernanceDomain. (The Console URLs are provided in Section 20.2, "About Identity and Access Management Console URLs.")
2. Navigate to **Environment -> Servers**.
3. Click **Lock and Edit**.

4. Click on the server **WLS_OIM1**.
5. Click on the **Server Start** subtab.
6. Add the following to the **Arguments** field:

   ```
   -Djava.net.preferIPv4Stack=true
   ```

7. Click **Save**.
8. Repeat Steps 4-7 for the managed server **WLS_OIM2**.
9. Click **Activate Changes**.

15.4.4 Configuring Oracle Identity Manager Servers to Listen on EoIB

This section is only required if the Oracle Identity Manager servers need to be accessed directly from outside the Exalogic machine. This is the case when external Oracle HTTP Servers are part of the configuration.

Create a new network channel as follows:

1. Log in to the WebLogic Console in the IAMGovernanceDomain.
2. Click **Lock & Edit**.
3. Navigate to **Environment -> Servers** to open the Summary of Servers page
4. In the Servers table, click **WLS_OIM1**.
5. Select **Protocols** and then **Channels**.
6. Click **New** to create a new channel.
7. Enter `OIMHOST1VHN-EXTCHAN` as the name. Select **HTTP** as the protocol and click **Next**.
8. In the Network Channel Addressing page, enter the following information:
   - **Listen Address**: `OIMHOST1VHN-EXT`

     This is the bond1 address assigned to OIMHOST1VHN-EXT
   - **Listen Port**: `8001`
9. Click **Next** and select the following in the Network Channel Properties page:
   - Enabled
   - HTTP Enabled for this protocol
10. Click **Finish**.
11. Click **Activate Changes**.

Repeat the preceding steps, substituting **WLS_OIM2** and `OIMHOST2VHN-EXT` for the Server and Listen Address.

15.5 Post-Deployment Steps for the Email Server

If you configured an email server in Section 13.12, "Configure Oracle Identity Manager" and the mail server security is SSL, follow these additional steps:

1. Ensure that the proxy is set for the environment

   a. Stop the **IAMGovernanceDomain** admin server and the OIM Managed Servers (**wls_oim1/2**).

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

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

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

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

For example:

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

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

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

   b. Remove this references from setDomainEnv.sh:

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

   c. Restart both the Administration and the Managed server.

15.6 Post-Deployment Steps for Access Manager

This section contains the following topics

- Section 15.6.1, "Modifying Access Manager Resources"
- Section 15.6.2, "Update Idle Timeout Value"
- Section 15.6.3, "Update WebGate Agents"

15.6.1 Modifying Access Manager Resources

During deployment, a number of resources are created in Access Manager with protection levels set. In order for Oracle Identity Manager to function correctly, one of these resources needs to be modified and one created.

To do this perform the following steps:

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.
5. Click the **Resources** tab.
6. Click New Resource and enter the following information:
   - **Type**: http

- **Description**: `provisioning-callback`
- **Host Identifier**: `IAMSuiteAgent`
- **Resource URL**: `/provisioning-callback/**`
- **Protection Level**: `Excluded`
- **Authentication Policy**: `n/a`
- **Authorization Policy**: `n/a`

7. Click **Apply**.
8. Locate the resource `/identity/**` by entering `/identity/*` in the Resource URL of the Resources search window.
9. Click **Edit**.
10. Change the **Protection Level** to **Excluded**.
11. Click **Apply**.

15.6.2 Update Idle Timeout Value

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

To update the idle timeout value:

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Log in as the Access Manager administrator user you created in Section 13.9, "Set User Names and Passwords" for example: `oamadmin`.
3. Click on **Common Settings** under **Configuration**.
4. Change **Idle Time out (minutes)** to `15`.
5. Click **Apply**.

15.6.3 Update WebGate Agents

After deployment, update existing WebGate Agents. The Identity and Access Management Console URLs are provided in Section 20.2, "About Identity and Access Management Console URLs."

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

To update these WebGate agents:

1. Log in to the Access Management Console as the Access Management administrator user identified by the entry in Section 13.9, "Set User Names and Passwords."
2. Click **SSO Agents** in the **Access Manager** box.
3. Ensure that the **WebGates** tab is selected.
4. Click **Search**.
5. Click an Agent, for example: **IAMSuiteAgent**.

6. Set the Security value to the same value defined to **OAM Transfer Mode** on the Access Manager Configuration screen in Section 13.15, "Configure Oracle Access Manager."

   The default setting is **Open** for AIX deployments and **Simple** for all others.

   Click Apply.

7. In the **Primary Server** list, click **+** and add any missing Access Manager Servers.

8. If a password has not already been assigned, enter a password into the **Access Client Password Field** and click **Apply**.

   Assign an Access Client Password, such as the **Common IAM Password** (*COMMON_IDM_PASSWORD*) you used in Section 13.9, "Set User Names and Passwords" or an Access Manager-specific password, if you have set one.

9. Set **Maximum Number of Connections** to 20 for all of the Access Manager Servers listed in the primary servers list. (This is the total maximum number of connections for the primary servers, which is 10 x WLS_OAM1 connections plus 10 x WLS_OAM2 connections.)

10. If you see the following in the **User Defined Parameters**:

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

    Change it to:

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

11. Click **Apply**.

12. Repeat Steps through for each WebGate.

13. Check that the security setting matches that of your Access Manager servers.

15.7 Enabling Exalogic Optimizations

Perform these steps to enable Exalogic optimizations:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Select **IAMAccessDomain** in the left navigation pane.
3. Click **Lock & Edit**.
4. On the Settings page, click the **General** tab.
5. Select **Enable Exalogic Optimizations**, and click **Save and Activate Changes**.
6. Repeat the steps for the **IAMGovernanceDomain**.
7. Restart the WebLogic Administration server.

15.8 Enabling Cluster-Level Session Replication Enhancements for Oracle Identity Manager and SOA

You can enable session replication enhancements for Managed Servers in a WebLogic cluster to which you will deploy a web application at a later time.

To enable session replication enhancements for `oim_cluster` in the domain `IAMGovernanceDomain`, use the values in the following table.

Table 15–1 Network Channel Properties

Managed Server	Name	Protocol	Listen Address	Listen Port	Additional Channel Ports
WLS_OIM1	`Replication Channel`	t3	OIMHOST1VHN.mycompany.com	7005	7006 to 7014
WLS_OIM2	`Replication Channel`	t3	OIMHOST2VHN.mycompany.com	7005	7006 to 7014
WLS_SOA1	`Replication Channel`	t3	SOAHOST1VHN.mycompany.com	7005	7006 to 7014
WLS_SOA2	`Replication Channel`	t3	SOAHOST2VHN.mycompany.com	7005	7006 to 7014

Proceed as follows:

1. Log in to the WebLogic Administration console at: `http://IGDADMIN.mycompany.com/console`
2. Ensure that Managed Servers in the `oim_cluster` cluster are up and running, as described in Section 20.1, "Starting and Stopping Components."
3. To set replication ports for a Managed Server, use the values in Table 15–1.

   To set the values for `WLS_OIM1`, for example, complete the following steps:

   a. Under **Domain Structure**, click **Environment** and **Servers**. The Summary of Servers page is displayed.

   b. Click **Lock & Edit**.

   c. Click `WLS_OIM1` on the list of servers. The Settings for WLS_OIM1 are displayed.

   d. Click the **Cluster** tab.

   e. In the **Replication Ports** field, enter a range of ports for configuring multiple replication channels. For example, replication channels for Managed Servers in `oim_cluster` can listen on ports starting from `7005` to `7015`. To specify this range of ports, enter `7005-7015`.

   f. Repeat Steps **a** through **e** for each of the other managed servers in Table 15–1.
4. The following steps show how to create a network channel for the managed server WLS_OIM1.

   a. Log in to the Oracle WebLogic Server Administration Console.

   b. If you have not already done so, click **Lock & Edit** in the Change Center.

   c. In the left pane of the Console, expand **Environment** and select **Servers**.

   The **Summary of Servers page** is displayed.

   d. In the Servers table, click **WLS_OIM1** Managed Server instance.

   e. Select **Protocols**, and then **Channels**.

   f. Click **New**.

   g. Enter **ReplicationChannel** as the name of the new network channel and select **t3** as the protocol, then click **Next**.

   h. Enter the following information:

Listen address: **OIMHOST1VHN.mycompany.com**

Note: This is the WLS_OIM1 floating IP assigned to WebLogic Server.

Listen port: **7005**

i. Click **Next**, and in the Network Channel Properties page, select **Enabled** and **Outbound Enabled**.

j. Click **Finish**.

k. Click **Save**.

l. Under the **Network Channels** table, select **ReplicationChannel**, the network channel you created for the `WLS_OIM1` managed server.

   Expand **Advanced**, select **Enable SDP Protocol**, and click **Save**.

m. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

You must repeat the above steps to create a network channel each for the remaining Managed Servers in the cluster. Enter the required properties, as described in Table 15–1.

5. After creating the network channel for each of the Managed Servers in your cluster, click **Environment** > **Clusters**. The Summary of Clusters page is displayed.
6. Click oim_cluster. The Settings for oim_cluster page is displayed.
7. Click the **Replication** tab.
8. In the **Replication Channel** field, ensure that `ReplicationChannel` is set as the name of the channel to be used for replication traffic.
9. In the **Advanced** section, select the **Enable One Way RMI for Replication** option.
10. Click **Save**.
11. Repeat these steps for the SOA cluster.
12. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

15.9 Add System Property Manually

Manually add the system property `-Djava.net.preferIPv4Stack=true` to the **startWebLogic.sh** script, which is located in the `bin` directory of *ASERVER_HOME*, using a text editor as follows:

1. Locate the following line in the startWebLogic.sh script:

```
. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
```

2. Add the following property immediately after the above entry:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.net.preferIPv4Stack=true"
```

3. Save the file and close.

Complete this procedure for each domain.

15.10 Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

This section describes how to configure single sign-on (SSO) for administration consoles in an Identity and Access Management Enterprise deployment.

This section includes the following topics:

- Section 15.10.1, "Overview of Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment"
- Section 15.10.2, "Setting Memory Parameters"
- Section 15.10.3, "Installing and Configuring WebGate 11g"
- Section 15.10.4, "Validating WebGate and the Access Manager Single Sign-On Setup"
- Section 15.10.5, "Updating OTD configuration Repository with Webgate Changes"
- Section 15.10.6, "Backing Up Single Sign-on"

15.10.1 Overview of Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

If you have not integrated Oracle Access Management Access Manager with Oracle Identity Manager, you must first create WebLogic Security Providers. Then proceed as follows.

You assign WebLogic Administration groups, update boot.properties, and restart the servers. Then you install and configure WebGate and validate the setup. After WebGate is installed and configured, the Oracle Traffic Director intercepts requests for the consoles and forwards them to Access Manager for validation.

The administration consoles referred to in the chapter title are:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console
- Oracle Access Management Console
- Oracle Identity Manager Console

15.10.2 Setting Memory Parameters

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

Setting the memory parameters is required only for the first start operation.

To edit the `setDomainEnv.sh` file to change memory allocation setting:

1. Open the `setDomainEnv.sh` file located in the following directory using a text editor:

   ```
   ASERVER_HOME/bin
   ```

2. Change the following memory allocation by updating the Java maximum memory allocation pool (Xmx) to `3072m` and initial memory allocation pool (Xms) to `1024m`.

   For example:

   ```
   WLS_MEM_ARGS_64BIT="-Xms1024m -Xmx3072m"
   ```

   or, in case of Oracle JRockit JVM:

   ```
   XMS_JROCKIT_64BIT="1024"
   XMX_JROCKIT_64BIT="3072"
   ```

   > **Note:** Change the values associated with the OS you are using.

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

   ```
   cd ASERVER_HOME/bin
   ./startWebLogic.sh
   ```

15.10.3 Installing and Configuring WebGate 11*g*

This section describes how to install and configure WebGate.

This section contains the following topics:

- Section 15.10.3.1, "Prerequisites"
- Section 15.10.3.2, "Installing Oracle WebGate on WEBHOST1 and WEBHOST2"

15.10.3.1 Prerequisites

Install and configure the Oracle Traffic Director as described in Section 12, "Installing and Configuring Oracle Traffic Director for an Enterprise Deployment," before installing the Oracle Web Gate:

15.10.3.2 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before starting the installer ensure that Java is installed on your machine. To install Oracle WebGate, run complete the following steps on WEBHOST1 and WEBHOST2. The WebGate installer can be found in: *`REPOS_HOME`*`/installers/webgate_otd`

1. Start the WebGate installer by issuing the command:

   ```
   ./runInstaller
   ```

   You are asked to specify the location of the Java Development Kit for example:

   `WEB_MW_HOME``/jrockit_`*`version`*

2. On the Welcome screen, click **Next**.
3. On the Install Software Updates screen, choose whether to skip updates, check with Oracle Support for updates, or search for updates locally.

   Click **Next**.
4. On the Specify Security Updates screen, specify these values:

   - **Email Address**: The email address for your My Oracle Support account.
   - **Oracle Support Password**: The password for your My Oracle Support account.

Select: **I wish to receive security updates via My Oracle Support**.

Click **Next**.

5. If the prerequisites fail because of missing 32-bit libraries, you can safely ignore this failure.
6. Click **Next**.
7. On the Installation Location Screen, enter the following information:

   Oracle Home Directory: *OTD_WEBGATE_ORACLE_HOME*

   Click **Next**.
8. On the installation summary screen, click **Install**.
9. Click **Next**.
10. Click **Finish**.
11. Execute the `deployWebGateInstance.sh` command from the following directory:

    ```
    OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/tools/deployWebGate
    ```

    Make sure this tool has executable permission.

    For example:

    ```
    OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/tools/deployWebGate
    ./deployWebGateInstance.sh -w LOCAL_CONFIG_DIR/webgate/ -oh OTD_WEBGATE_ORACLE_
    HOME -ws otd
    ```

    Expected output:

    ```
    Copying files from WebGate Oracle Home to WebGate Instancedir
    ```

    Note: The deployment directory must be the same on every host.

12. Set the environment variable LD_LIBRARY_PATH to:

    ```
    OTD_WEBGATE_ORACLE_HOME/lib
    ```

    For example:

    ```
    export LD_LIBRARY_PATH=WEB_ORACLE_HOME/webgate/lib
    ```

13. Edit the properties in the `sso.mycompany.com-obj.conf` and `admin.mycompany.com-obj.conf` files using the `EditObjConf` tool located in the following directory:

    ```
    OTD_WEBGATE_ORACLE_HOME/webgate/iplanet/tools/setup/InstallTools
    ```

    For example, on WEBHOST1, run the following:

    ```
    ./EditObjConf -f WEB_ORACLE_INSTANCE/net-IDM/config/sso.mycompany.com-obj.conf
    -oh OTD_WEBGATE_ORACLE_HOME -w LOCAL_CONFIG_DIR/webgate -ws otd

    ./EditObjConf -f WEB_ORACLE_
    INSTANCE/net-IDM/config/iadadmin.mycompany.com-obj.conf -oh OTD_WEBGATE_ORACLE_
    HOME -w LOCAL_CONFIG_DIR/webgate -ws otd

    ./EditObjConf -f WEB_ORACLE_
    INSTANCE/net-IDM/config/igdadmin.mycompany.com-obj.conf -oh OTD_WEBGATE_ORACLE_
    ```

```
HOME -w LOCAL_CONFIG_DIR/webgate -ws otd

./EditObjConf -f WEB_ORACLE_
INSTANCE/net-IDM/config/idminternal.mycompany.com-obj.conf -oh OTD_WEBGATE_
ORACLE_HOME -w LOCAL_CONFIG_DIR/webgate -ws otd
```

Expected output:

```
WEB_ORACLE_INSTANCE/config/magnus.conf has been backed up as WEB_ORACLE_
INSTANCE/config/magnus.conf.ORIG
WEB_ORACLE_INSTANCE/config/instance_config_name-obj.conf has been backed up as
WEB_ORACLE_INSTANCE/instance_config_name-obj.conf.ORIG
```

14. Register WebGate to the Access Manager 11g Server by copying the WebGate artifacts Located in the following directory:

    ```
    IAD_ASERVER_HOME/output/Webgate_IDM_11g
    ```

    to the following directories.

    Copy aaa_cert.pem and aaa_key.pem to:

    ```
    LOCAL_CONFIG_DIR/webgate/webgate/config/simple
    ```

    Copy cwallet.sso, ObAccessClient.xml and password.xml to:

    ```
    LOCAL_CONFIG_DIR/webgate/webgate/config
    ```

    To copy the artifacts run the following commands:

    ```
    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/aaa* to LOCAL_CONFIG_
    DIR/webgate/webgate/config/simple

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/password.xml to LOCAL_CONFIG_
    DIR/webgate/webgate/config/

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/ObAccessClient.xml to LOCAL_CONFIG_
    DIR/webgate/webgate/config/

    cp IAD_ASERVER_HOME/output/Webgate_IDM_11g/cwallet.sso to LOCAL_CONFIG_
    DIR/webgate/webgate/config/
    ```

15. Add LD_LIBRARY_PATH to Oracle Traffic Director Start Scripts.

    To prevent you having to enter the LD_LIBRARY_PATH each time you start Oracle traffic Director, add it to the OTD start script:

    a. Edit the `startserv` file located in the following directory

       ```
       WEB_ORACLE_INSTANCE/net-IDM/bin
       ```

    b. Locate the following line:

       ```
       # Set LD_LIBRARY_PATH for Solaris and Linux
       LD_LIBRARY_PATH="${SERVER_LIB_PATH}:${LD_LIBRARY_PATH}"; export LD_LIBRARY_
       PATH
       ```

    c. Add the following line immediately after:

       ```
       LD_LIBRARY_PATH=$LD_LIBRARY_PATH:OTD_WEBGATE_ORACLE_HOME/lib:${LD_LIBRARY_
       PATH}; export LD_LIBRARY_PATH
       ```

       After editing, the file appears as follows:

```
# Set LD_LIBRARY_PATH for Solaris and Linux

LD_LIBRARY_PATH="${SERVER_LIB_PATH}:${LD_LIBRARY_PATH}"; export LD_LIBRARY_
PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:OTD_WEBGATE_ORACLE_HOME/lib:${LD_LIBRARY_
PATH}; export LD_LIBRARY_PATH
```

   d. Save this file.

16. Repeat this procedure for each WEBHOST.

> **Note:** Configuring WebGate in this way directly modifies the Oracle Traffic Director configuration files. These changes are not reflected in the OTD configuration store. The next time you go into OTD and modify the configuration, OTD it will indicate that there is a discrepancy between that config store and the values on disk. It will ask you what you want to do. YOU MUST tell OTD to pull the configuration from the files rather than push the configuration back to the files. Selecting the wrong option will remove the WebGate configuration you just performed.

15.10.3.3 Restarting the Oracle Traffic Director Instance

Use the `startserv` command to start or `stopserv` command to stop your Oracle Traffic Director instance.

If you did not install Oracle Traffic Director as root. Stop the failover groups using the following command as root:

```
OTD_ORACLE_HOME/bin/tadm stop-failover --instance-home=WEB_INSTANCE_HOME/
--config=sso.mycompany.com
```

To stop the server, run the following command:

```
WEB_ORACLE_INSTANCE/net-IDM/bin/stopserv
```

To start the server, run the following command:

```
export LD_LIBRARY_PATH=OTD_WEBGATE_ORACLE_HOME/lib
WEB_ORACLE_INSTANCE/net-IDM/bin/startserv
```

If you did not install Oracle Traffic Director as root. Start the failover groups using the following command as root:

```
OTD_ORACLE_HOME/bin/tadm start-failover --instance-home=WEB_INSTANCE_HOME/
--config=sso.mycompany.com
```

To restart the Oracle Traffic Director instance, stop all running instances, and then run the start command.

15.10.3.4 Add LD_LIBRARY_PATH to OTD Start Scripts

To prevent you having to enter the `LD_LIBRARY_PATH` each time you start OTD, you can add it to the OTD start script.

To do this, proceed as follows:

1. Edit the file `startserv`, which is located in the directory: *WEB_ORACLE_INSTANCE*`/net-IDM/bin`
2. Locate the line that looks like this:

```
# Set LD_LIBRARY_PATH for Solaris and Linux
LD_LIBRARY_PATH="${SERVER_LIB_PATH}:${LD_LIBRARY_PATH}"; export LD_LIBRARY_PATH
```

3. Add the following line afterwards:

```
LD_LIBRARY_PATH=$LD_LIVRARY_PATH:OTD_WEBGATE_ORACLE_HOME/lib; export LD_
LIBRARY_PATH
```

4. Save the file.

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

To validate that WebGate is functioning correctly, open a web browser and go the Access Management Console URL listed in Section 20.1, "Starting and Stopping Components."

You now see the Oracle Access Management Login page displayed. Enter your Access Manager administrator user name (for example, oamadmin) and password and click **Login**. Then you see theOracle Access Management console displayed.

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console and to Oracle Enterprise Manager Fusion Middleware Control at the URLs listed in Section 20.2, "About Identity and Access Management Console URLs."

The Oracle Access Management Single Sign-On page displays. Provide the credentials for the weblogic_idm user to log in.

15.10.5 Updating OTD configuration Repository with Webgate Changes

The commands in previous sections manually update the Oracle Traffic Director configuration files. After the files are updated, the OTD configuration is inconsistent with the information in the files. Subsequent deployments would therefore erase the new configuration. Therefore, you must update the OTD configuration with the manual changes made in the previous sections.

To update the OTD configuration:

1. Log in to the OTD Administration Console using the following URL:

   ```
   https://OTDADMINVHN:OTD_ADMIN_PORT
   ```

2. Click the **Deploy** button at the top of the screen.

   A message box appears stating that the administration server has detected configuration modifications on some instances.

3.

4. Select the option **Pull and deploy configuration** and click **OK**.

   And click OK

15.10.6 Backing Up Single Sign-on

Back up the Web Tier and WebLogic domain, as described in Section 20.5, "Performing Backups and Recoveries."

15.11 Enable SDP Support for JDBC Connections

If you Exalogic Machine is connected to an Exadata Machine which is hosting your database, you must update your JDBC connections to utilise the SDP protocol. Then you must tell the managed servers that SDP is in use. Proceed as follows:

> **Note:** Perform the steps below for each datasource in each domain that accesses the database using SDP.

1. Log into the WebLogic Administration console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Lock and Edit**.
3. Expand **Services** in the Domain Structure window.
4. Click **Data sources**.
5. Click on a data source, for example: **oamDS**.
6. Select the **Connection Pool** tab.
7. Update the value of the URL. Instead of using SCAN and TCP, the URL should be an SDP connection to the listeners on each of the Database Servers.

   For example, if the TCP URL is of the form:

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
   LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN)(PORT=1521)))(CONNECT_
   DATA=(SERVICE_NAME=oamedg.mycompany.com)))
   ```

   Change it to:

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=
   (ADDRESS=(PROTOCOL=SDP)(HOST=IAMDBHOST01ib-vip.mycompany.com)(PORT=1522))
   (ADDRESS=(PROTOCOL=SDP)(HOST=IAMDBHOST02ib-vip.mycompany.com)(PORT=1522)))
   (CONNECT_DATA=(SERVICE_NAME=oamedg.mycompany.com)))
   ```

   In this case, IAMDBHOST01ib-vip and IAMDBHOST02ib-vip are the listen addresses on the individual RAC nodes. The HOST and PORT should correspond to those of the IB Listener on each machine.
8. Click **Save**.
9. Repeat for each data source.

   Now that the JDBC data sources have been updated, tell the managed servers that SDP is in use.

Now that the JDBC data sources have been updated, tell the managed servers that SDP is in use, as follows:

1. Expand **Environment** from the **Domain Structure** menu.
2. Click **Servers**. The Server summary page is displayed.
3. Click on a server name, for example: **AdminServer**

> **Note:** If you are intending to start your administration server using the `startWeblogic.sh` script, also add this parameter to that file in the `JAVA_OPTIONS`.

4. Click on the server start sub tab
5. Add the following to the arguments field if not already present:

   ```
   -Doracle.net.SDP=true -Djava.net.preferIPv4Stack=true
   ```

6. Click **Save**.
7. Repeat for each Managed Server.
8. When finished, click **Activate Changes**.

   Validate the data sources connection, after restarting all components, as described in section Section 15.13, "Restarting All Components."

   Through the WebLogic Administration Console, using the steps described in Section 15.11, "Enable SDP Support for JDBC Connections," select **Services**, **Data Sources**, **Data Source**, the **Monitoring** tab, and then the **Testing** subtab.

   Select a server from the list and click **Test Data Source**.

   The response should be successful.

15.12 Adding a Load Balancer Certificate to Trust Stores

SSL certificates used by the load balancer must be added to the trusted certificates in the JDK.

To add the certificate:

1. Obtain the certificate from the load balancer.

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

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

   For example:

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

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

   ```
   SHARED_CONFIG_DIR/keystores
   ```

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

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

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

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

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

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

keytool -importcert -file SHARED_CONFIG_DIR/keystores/sso.mycompany.com.pem
-trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2.mycompany.com.jks
```

Where JAVA_HOME is set to IGD_MW_HOME/jdk6

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

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

15.13 Restarting All Components

Restart all components, as described in Section 20.1, "Starting and Stopping Components."

16 Validating Deployment

The Deployment process includes several validation checks to ensure that everything is working correctly. This chapter describes additional checks that you can perform for additional sanity checking.

This chapter contains the following sections:

- Section 16.1, "Validating the Administration Server"
- Section 16.2, "Validating the Access Manager Configuration"
- Section 16.3, "Validating Oracle Identity Manager"
- Section 16.4, "Validating SOA Instance from the WebTier"
- Section 16.5, "Validating Oracle Unified Directory"
- Section 16.6, "Validating WebGate and the Access Manager Single Sign-On Setup"

16.1 Validating the Administration Server

Validate the WebLogic Administration Server as follows.

16.1.1 Verify Connectivity

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

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

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

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

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

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

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

16.1.2 Validating Failover

Test failover of the Access Administration server to OAMHOST2, and then fall back to OAMHOST1 as described in Section 20.8, "Manually Failing Over the WebLogic Administration Server."

Test failover of the Identity Governance Administration server to OIMHOST2, and then fall back to OIMHOST1 as described in Section 20.8, "Manually Failing Over the

WebLogic Administration Server."

16.2 Validating the Access Manager Configuration

To Validate that this has completed correctly.

1. Access the Access Management Console at: `http://IADADMIN.mycompany.com/oamconsole`
2. Log in as the `oamadmin` user or the user identified by the entry in Section 13.9, "Set User Names and Passwords."
3. Click the **System Configuration** tab
4. Click **SSO Agents** in the **Access Manager** section.
5. Click **Search**.
6. You should see the WebGate agents `Webgate_IDM`, `Webgate_IDM_11g`, `IAMSuiteAgent`, and `accessgate-oic`.

16.3 Validating Oracle Identity Manager

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

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

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

Log in using the `xelsysadm` username and password.

16.4 Validating SOA Instance from the WebTier

Validate SOA by accessing the URL:

```
http://IDMINTERNAL.mycompany.com:7777/soa-infra
```

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

> **Note:** You may need to add soa-infra as an excluded resource in OAM.

16.5 Validating Oracle Unified Directory

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

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

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

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

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

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

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

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

- Automatically trust
- Use a truststore
- Manually validate

Select your choice.

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

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

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

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

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

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

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

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

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

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

Enterprise Manager Fusion Middleware Control at:

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

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

16.7 Validating the Deployment

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

Testing SSO

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

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

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

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

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

Creating a New User in OUD to be Used by OAM

To create a new user in OUD:

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

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

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

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

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

Testing the SOA workflow for approvals

To test the SOA workflow for approvals:

1. Access a protected resource, such as:

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

2. Click **Register New Account**.
3. Complete information about the new account and click **Register**
4. Click **Return**, then make a note of the request number.
5. Log in to the Oracle Identity Self Service as the user `xelsysadm`.
6. Click **Inbox**.

7. You request appears in the list of Pending approvals.
8. Click on the request and select **Approve** from the **Actions** menu.
9. Log out of the Oracle Identity Self Service.
10. Log back in as the newly created user.

17

Extending the Domain to Include Oracle Adaptive Access Manager

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

This chapter contains the following topics:

17.1 Overview of Extending the Domain to Include Oracle Adaptive Access Manager

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

Oracle Adaptive Access manager consists of the following two components.

- OAAM Administration Applications
- OAAM Server Applications

17.2 OAAM Details

Use this worksheet to keep track of OAAM information

Table 17–1 OAAM Details

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

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

17.3 Prerequisites

The instructions in the following subsections are for the Exalogic virtual mode. If you are using the Exalogic physical deployment, references to OAMHOST1 and OAMHOST2 should be replaced by IAMHOST1 and IAMHOST2, as shown in Table 17–1.

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

17.3.1 Creating a Highly Available Database

Create a highly available database to hold the OAAM data, if you are not using the IAMDB. Pre-seed the database with OAAM data objects using the repository creation utility as described in Section 10.5, "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU."

17.3.2 Creating OAAM Users and Groups in LDAP

Create OAAM Users and Groups as follows:

Create a configuration file with the following contents:

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

Where:

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

  OUD: LDAPHOST1 and 1389

- IDSTORE_ADMIN_PORT (*LDAP_DIR_ADMIN_PORT*) is the administration port of your Oracle Unified Directory instance.
- IDSTORE_BINDDN (*LDAP_ADMIN_USER*) is an administrative user in the Identity Store Directory.
- IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored. This is composed of cn=Groups combined with the *REALM_DN* defined in Section 11.1, "Assembling Information for Identity and Access Management Deployment," for example: cn=Groups,dc=mycompany,dc=com
- IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored. This is the same as the *REALM_DN* defined in Section 11.1, "Assembling Information for Identity and Access Management Deployment," for example: dc=mycompany,dc=com
- IDSTORE_USERNAMEATTRIBUTE is the name of the directory attribute containing the user's name, for example: cn. Note that this is different from the login name.

- IDSTORE_LOGINATTRIBUTE is the LDAP attribute which contains the users Login name, for example: uid.
- IDSTORE_USERSEARCHBASE is the location in the directory where users are stored. This is composed of cn=Users combined with the *REALM_DN* defined in Section 11.1, "Assembling Information for Identity and Access Management Deployment," for example: cn=Users,dc=mycompany,dc=com
- IDSTORE_OAAMADMINUSER (*OAAMADMINUSER*) is the name of the user you want to create as your Oracle Adaptive Access Manager Administrator.

Create users using idmConfigTool.

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

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

   The syntax of the command on Linux is:

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

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

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

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

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

17.4 Extending Domain for Oracle Adaptive Access Manager

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

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

Then proceed as follows:

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

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

- **Oracle Adaptive Access Manager - Admin Server**

   Click **Next**

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

   Select:

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

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

   Click **Next**.

5. The Gridlink RAC Component Schema screen appears. In this screen, enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU. For Exadata SDP Connections, enter the TCP parameters below. Later, this must be converted to an SDP Connect String.

   - **Driver**: Select Oracle's driver (Thin) for GridLink Connections,Versions:10 and later.
   - Select **Enable FAN**.
   - Do one of the following:
     - If SSL is not configured for ONS notifications to be encrypted, deselect **SSL**.
     - Select **SSL** and provide the appropriate wallet and wallet password.
   - **Service Listener**: Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the parameter `remote_listener` in the database:

     ```
     SQL>show parameter remote_listener;

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

     Note:

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

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

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

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

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

and

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

Use the screen at the top left side of the wizard to update the values reflected on the lower bottom screen. Once the value of a row is updated, it has to be deselected to enter the value for the next row. Otherwise, the value is overwritten.

Enter the following RAC component schema information:

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

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

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

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

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

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

Default Name	Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
	wls_oaam_admin2	*OAMHOST2*	14200 (*OAAM_PORT*)	14201 (*OAAM_SSL_PORT*)	Selected

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

[2] See Section B.3.

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

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

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

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

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

Assign servers to the clusters as follows:

Cluster	Server
oaam_cluster	wls_oaam1
	wls_oaam2
oaam_admin_cluster	wls_oaam_admin1
	wls_oaam_admin2

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

Click **Next**.

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

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

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

- **OAMHOST1**: **wls_oaam1**, **wls_oaam_admin1**
- **OAMHOST2**: **wls_oaam2**, **wls_oaam_admin2**

Click **Next** to continue.

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

> **Note:** Note: If you receive a warning that says:
>
> ```
> CFGFWK: Server listen ports in your domain configuration conflict
> with ports in use by active processes on this host
> ```
>
> Click **OK**.
>
> This warning appears if Managed Servers have been defined as part of previous installs and can safely be ignored.

17.5 Restarting Administration Server on OAMHOST1

Restart WebLogic Administration Server on OAMHOST 1. See Section 20.1, "Starting and Stopping Components."

17.6 Deploying Managed Server Configuration to Local Storage

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

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

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

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

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

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

   This creates a file called `iam_domain.jar`.

   > **Note:** The template is common to both hosts as it is mounted and available on the other host.

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

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

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

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

17.7 Adding OAAM Servers to Start and Stop Scripts

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

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

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

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

For example:

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

For each of the OAAM managed servers in the table in Section 17.4, "Extending Domain for Oracle Adaptive Access Manager", Step 8 (Configure Managed Servers screen), add an entry which looks like this:

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

For example:

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

Save the file.

17.8 Starting and Validating OAAM on OAMHOST1

This section contains the following topics:

- Section 17.8.1, "Starting Oracle Adaptive Access Manager on OAMHOST1"
- Section 17.8.2, "Validating OAAM on OAMHOST1"

17.8.1 Starting Oracle Adaptive Access Manager on OAMHOST1

Start the WebLogic Administration Console for `IAMAccessDomain` using the URL specified in Section 20.2, "About Identity and Access Management Console URLs."

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

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

17.8.2 Validating OAAM on OAMHOST1

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

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

and to the OAAM server at:

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

The implementation is valid if the OAAM Server login page is displayed and you can log in using the `oaamadmin` account you created in Section 17.3.2, "Creating OAAM Users and Groups in LDAP."

17.9 Starting and Validating OAAM on OAMHOST2

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

This section contains the following topics:

- Section 17.9.1, "Starting Oracle Adaptive Access Manager on OAMHOST2"
- Section 17.9.2, "Validating OAAM on OAMHOST2"

17.9.1 Starting Oracle Adaptive Access Manager on OAMHOST2

Start Oracle Adaptive Access Manager on OAMHOST2 by following the start procedures in Section 20.1, "Starting and Stopping Components" for WebLogic Managed Servers wls_oaam2 and wls_oaam_admin2.

17.9.2 Validating OAAM on OAMHOST2

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

```
http://OAMHOST2.mycompany.com:14200/oaam_admin
```

and to the OAAM server at:

```
http://OAMHOST2.mycompany.com:14300/oaam_server
```

The implementation is valid if the OAAM Server login page is displayed and you can log in using the `oaamadmin` account you created in Section 17.3.2, "Creating OAAM Users and Groups in LDAP."

17.10 Configuring OAAM to Work with Web Tier

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

> **Note:** If you are using Oracle Traffic Director, follow Section 17.10.1, "Configuring Access from Oracle Traffic Director." If you are using external Oracle HTTP Server, follow Section 17.10.2, "Configuring Access from Oracle HTTP Server."

This section contains the following topics:

- Section 17.10.1, "Configuring Access from Oracle Traffic Director"
- Section 17.10.2, "Configuring Access from Oracle HTTP Server"
- Section 17.10.3, "Changing Host Assertion in WebLogic"
- Section 17.10.4, "Validating Oracle Adaptive Access Manager"

17.10.1 Configuring Access from Oracle Traffic Director

Create a server pool for OAAM Managed Servers as described in Section 12.7.1, "Creating an Origin-Server Pool."

Create OTD routes for OAAM as described in Section 12.8, "Creating Routes."

17.10.2 Configuring Access from Oracle HTTP Server

If you are adding OAAM to an existing domain, you must include OAAM in the Oracle HTTP Server configuration by updating the following files on WEBHOST1 and WEBHOST2. Depending on whether or not you are using OTD or the Oracle HTTP server to serve your web requests the instructions for incorporating OAAM into the web tier are different.

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

17.10.2.1 Updating IADADMIN.mycompany.com

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

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

   # OAAM Console
   <Location /oaam_admin>
      SetHandler weblogic-handler
      WebLogicCluster OAMHOST1.mycompany.com:14200,OAMHOST2.mycompany.com:14200
   </Location>
```

17.10.2.2 Updating sso.mycompany.com

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

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

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

17.10.2.3 Restarting Oracle HTTP Servers and OAAM Managed Servers

Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2, as described in Section 20.1, "Starting and Stopping Components."

Restart the managed servers wls_oaam1, wls_oaam2, wls_oaam_admin1, and wls_oaam_admin2 as described in Section 20.1, "Starting and Stopping Components."

17.10.3 Changing Host Assertion in WebLogic

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

To do this, log in to the WebLogic administration console in the IAMAccessDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."

Then proceed as follows:

1. Select **Clusters** from the home page or, alternatively, select **Environment** -> **Clusters** from the Domain structure menu.
2. Click **Lock and Edit** in the Change Center Window to enable editing.
3. Click the Cluster Name (**oaam_cluster**).
4. Select **HTTP** and enter the following values (from Section 11.1, "Assembling Information for Identity and Access Management Deployment"):

   - **Frontend Host**: `sso.mycompany.com` (*`IAM_LOGIN_URI`*)
   - **Frontend HTTP Port:** `80` (*`HTTP_PORT`*)
   - **Frontend HTTPS Port:** `443` (*`HTTP_SSL_PORT`*)

   This ensures that any HTTPS URLs created from within WebLogic are directed to port 443 on the load balancer.
5. Click **Save**.
6. Select **Clusters** from the home page or, alternatively, select **Environment** -> **Clusters** from the Domain structure menu.
7. Click the Cluster Name (**oaam_admin_cluster**).
8. Select HTTP and enter the following values (from Section 11.1, "Assembling Information for Identity and Access Management Deployment"):

   - **Frontend Host**: `IADADMIN.mycompany.com` (*`IAD_DOMAIN_ADMIN_LBRVHN`*)
   - **Frontend HTTP Port**: `80` (*`HTTP_PORT`*)
9. Click **Save**.
10. Click **Activate Changes** in the Change Center window to enable editing.
11. Restart the managed servers.

17.10.4 Validating Oracle Adaptive Access Manager

Log in to the Oracle Adaptive Access Management Administration console, at the URL listed in Section 20.2, "About Identity and Access Management Console URLs," using the `oaamadmin` account you created in Section 13.5.2, "Creating OAAM Administration User in WebLogic Console."

Also log in to the Oracle Adaptive Access Manager server at `https://sso.mycompany.com/oaam_server` in using the account `oaamadmin` account and the password `test`.

Check that the following URL can be accessed:

```
https://sso.mycompany.com:443/oaam_server/oamLoginPage.jsp
```

Note: The credential collection procedure is the same in Exalogic and Non-Exalogic deployments, but after the credential collection page is displayed you see a "Page not found error" in the Exalogic test. This is normal and occurs because there is no such page in Oracle Traffic Director.

17.11 Loading Oracle Adaptive Access Manager Seed Data

This section describes how to load seed data into Oracle Adaptive Access Manager.

Note: Either copy the files from OAMHOST1 to your local machine (where you are running the browser) or run this step from a browser started on OAMHOST1.

1. Log in to Oracle Adaptive Access Management Administration console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."

   Connect using the `oaamadmin` account that you created in Section 17.3.2, "Creating OAAM Users and Groups in LDAP."

2. Click **System Snapshots**, which is located on the **Navigation -> Environment** menu.

   Click **List System Snapshots**.

3. Click **Load From File**.

4. Enter the following information:

   - **Name**: `Default Snapshot`
   - **Notes**: `Default Snapshot`

   Select **Backup Current System Now**.

   Click **Continue**.

5. Click **OK** to acknowledge backup creation.

6. Click **Choose File.**

7. Select the file `oaam_base_snapshot.zip` which is located in:

   ```
   IAD_ORACLE_HOME/oaam/init
   ```

8. Click **Load**.

   You will see a message that says that the snapshot file was loaded successfully. Acknowledge this message by clicking **OK**.

9. Click **Restore** near the top right.

10. When loading is complete, a message is displayed. Click **OK**.

17.12 Integrating Oracle Adaptive Access Manager with Oracle Access Management Access Manager

This section describes how to integrate OAAM with Access Manager and Oracle Identity Manager. Once OAAM has been integrated with Access Manager, you can use OAAM instead of the standard Access Manager login to validate access to resources.

Even though OAAM is performing the authentication, it is authenticating against users in Access Manager.

When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

This section contains the following topics:

- Section 17.12.1, "Retrieving the Global Passphrase for Simple Mode."
- Section 17.12.2, "Registering OAAM as a Third Party Application."
- Section 17.12.3, "Setting OAAM properties for Access Manager."
- Section 17.12.4, "Creating Oracle Adaptive Access Manager Policies."
- Section 17.12.5, "Creating a Resource in Access Manager,"
- Section 17.12.6, "Moving TAP Resource to LDAP Policy,"
- Section 17.12.7, "Validating the Integration."

17.12.1 Retrieving the Global Passphrase for Simple Mode

Access Manager generates a random global passphrase for Simple mode communication during installation. The following procedure describes how to retrieve this passphrase. You will need it later in this chapter.

To retrieve the random global passphrase for Simple mode communication, on OAMHOST1 invoke the WebLogic Scripting Tool located in `*IAD_ORACLE_HOME*/common/bin`. Once you are in the `wlst` shell, enter the command to connect.

```
./wlst.sh
wls:/offline> connect()
```

Respond to the prompts as shown:

```
Please enter your username [weblogic] : weblogic
Please enter your password [weblogic] : COMMON_IDM_PASSWORD
Please enter your server URL [t3://localhost:7001] : t3://IADADMINVHN:7001
wls:/IAMAccessDomain/serverConfig>
```

Enter the following command to change the location to the read-only domainRuntime tree. For help, use `help(domainRuntime))`.

```
wls:/IAMAccessDomain/domainRuntime>domainRuntime()
```

View the global passphrase by entering the following command.

```
wls:/IAMAccessDomain/domainRuntime> displaySimpleModeGlobalPassphrase()
```

Make a note of this passphrase and exit `wlst` by using the `exit` command:

```
wls:/IAMAccessDomain/domainRuntime> exit()
```

17.12.2 Registering OAAM as a Third Party Application

If you have configured Access Manager to use the Simple Security Transportation protocol, you must register OAAM as a third-party application.

To register OAAM as a third-party application:

1. Create a directory to hold the OAAM Keystore. Placing this directory in the *IAD_ASERVER_HOME* ensures that it is available to all OAAM Hosts.

```
mkdir -p IAD_ASERVER_HOME/keystores
```

2. From OAMHOST1, start the WLST shell from the *IAD_ORACLE_HOME*/common/bin directory. For example, on Linux, you would type:

   ```
   ./wlst.sh
   ```

3. Connect to the WebLogic Administration Server using the following `wlst` connect command:

   ```
   connect('AdminUser',"AdminUserPassword",t3://hostname:port')
   ```

   For example:

   ```
   connect("weblogic","admin_password","t3://IADADMINVHN.mycompany.com:7001")
   ```

4. Run the `registerThirdPartyTAPPartner` command as follows:

   ```
   registerThirdPartyTAPPartner(partnerName = "partnerName", keystoreLocation=
   "path to keystore" , password="keystore password", tapTokenVersion="v2.0",
   tapScheme="TAPScheme", tapRedirectUrl="OAAM login URL")
   ```

   For example:

   ```
   registerThirdPartyTAPPartner(partnerName = "OAAMTAPPartner", keystoreLocation=
   "IAD_ASERVER_HOME/keystores/oaam_keystore.jks" , password="password",
   tapTokenVersion="v2.0", tapScheme="TAPScheme",
   tapRedirectUrl="https://sso.mycompany.com/oaam_server/oamLoginPage.jsp")
   ```

   Where:

   - `partnerName` is a unique name. If the partner exists in Access Manager, the configuration will be overwritten.
   - `keystoreLocation` is an existing Key Store location. If the directory path you specified is not present, you get an error.
   - `password` is the password specified to encrypt the key store. Remember this, as you will need it later.
   - `tapTokenVersion` is always `v2.0`.
   - `tapScheme` is the authentication scheme to be updated.
   - `tapRedirectUrl` is a reachable URL. If it is not, registration fails with the message: `Error! Hyperlink reference not valid.`

     Note: Due to a bug, `tapRedirectURL` must be an HTTP URL. This is changed to HTTPS later.

   - `tapRedirectUrl` is:

     ```
     https://sso.mycompany.com/oaam_server/oamLoginPage.jsp
     ```

5. Exit WLST.

   ```
   exit()
   ```

6. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."

7. Click **Authentication Schemes** in the **Access Manager** section.

The Search Authentication Schemes Page is displayed.

Enter `TAPScheme` in the **Search Name** box and click **Search**.

8. Click **TAPScheme**.
9. Verify that the **Challenge URL** is set to:

   `/oaam_server/oamLoginPage.jsp`

   The parameters `TAPPartnerId=OAAMTAPPartner` and `SERVER_HOST_ALIAS=OAMSERVER` should already be listed as **Challenge Parameter**s. Add the following **Challenge Parameter**s:

   - `MatchLDAPAttribute=uid`
   - `TAPOverrideResource=https://sso.mycompany.com:443/oamTAPAuthenticate`
10. Click **Apply**.
11. Restart wls_oaam1 and wls_oaam2 as described in Section 20.1, "Starting and Stopping Components."

17.12.3 Setting OAAM properties for Access Manager

Set the OAAM properties for Access manager by editing the `oaam_cli.properties` file.

To set the OAAM properties on OAMHOST1:

1. Copy *`IAD_ORACLE_HOME`*`/oaam/cli` to a temporary location. For example:

   ```
   cp -r IAD_ORACLE_HOME/oaam/cli/u01/oracle/oaam
   ```

2. Edit the file `oaam_cli.properties`, which is located in the directory:

   `/u01/oracle/oaam/conf/bharosa_properties`.

   Set the following property values in the file:

Parameter	Value
`oaam.adminserver.hostname`	`IADADMINVHN.mycompany.com`
`oaam.adminserver.port`	`7001`
`oaam.adminserver.username`	`weblogic`
`oaam.adminserver.password`	Password for the `weblogic` user
`oaam.db.url`	The DBC URL for the OAAM Database. Format: `jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=oaamedg.mycompany.com)))`
`oaam.uio.oam.tap.keystoreFile`	The location of the keystore that was created in Section 17.12.2, "Registering OAAM as a Third Party Application."For example: *`IAD_ASERVER_HOME`*`/keystores/oaam_keystore.jks`
`oaam.uio.oam.tap.partnername`	`OAAMTAPPartner`
`oaam.uio.oam.host`	*`OAMHOST1`*
`oaam.uio.oam.port`	The Access Manager Server proxy port *`OAM_PROXY_PORT`*. For example: `5575`.
`oaam.uio.oam.webgate_id`	`IAMSuiteAgent`
`oaam.uio.oam.secondary.host`	*`OAMHOST2`*

Parameter	Value
`oaam.uio.oam.secondary.host.port`	The Access Manager Server proxy port, *`OAM_PROXY_PORT`*, on the second Access Manager Server. For example: `5575`.
`oaam.uio.oam.security.mode`	This depends on the Access Manager security transport mode in use. If this is an AIX build, then the value will be `1` (Open) otherwise it will be `2` (Simple).
`oam.uio.oam.rootcertificate.keystore.filepath`	The location of the Keystore file generated for the root certificate: *`IAD_ASERVER_HOME`*`/output/webgate-ssl/oamclient-truststore.jks` This is required only for security modes `2` (Simple) and `3` (Cert).
`oam.uio.oam.privatekeycertificate.keystore.filepath`	The location of the Keystore file generated for private key: *`IAD_ASERVER_HOME`*`/output/webgate-ssl/oamclient-keystore.jks` This is required for security modes `2` (Simple) and `3` (Cert).

Save the file

3. Execute the OAAM CLI tool by issuing the command `setupOAMTapIntegration.sh`, which is located in the directory:

   `/u01/oracle/oaam`

   as follows:

   Set `ORACLE_MW_HOME` to *`IAD_MW_HOME`*

   Set `JAVA_HOME` to *`JAVA_HOME`*

   Set `WLS_HOME` to *`IAD_MW_HOME`*`/wlserver_10.3`

   Set `APP_SERVER_TYPE` to `weblogic`

   Run the commands:

```
chmod +x /u01/oracle/oaam/setupOAMTapIntegration.sh
/u01/oracle/oaam/setupOAMTapIntegration.sh /u01/oracle/oaam/conf/bharosa_
properties/oaam_cli.properties
```

   When the command runs, it prompts you for the following information:

   - OAAM AdminServer User Name: `weblogic`
   - OAAM AdminServer Password: Password for `weblogic` account
   - OAAM DB username: `EDGIAD_OAAM`.
   - OAAM DB password: Password for the OAAM database user.
   - OAM Webgate Credentials to be stored in CSF: Enter WebGate password (*`COMMON_IDM_PASSWORD`*).
   - OAM TAP Key store file password: The password you assigned when you registered OAAM as a 3rd party application in Section 17.12.2, "Registering OAAM as a Third Party Application" (*`COMMON_IDM_PASSWORD`*).
   - OAM Private Key certificate Key store file password: The Access Manager global passphrase obtained in Section 17.12.1, "Retrieving the Global Passphrase for Simple Mode."
   - OAM Global Pass phrase: If you are using the OAAM Simple security model then this is the value retrieved in Section 17.12.1, "Retrieving the Global Passphrase for Simple Mode."

17.12.4 Creating Oracle Adaptive Access Manager Policies

Create a group for OAAM Protected resources in the IAMSuite Application Domain.

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs," using the `oamadmin` account created previously
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**. The IAM Suite Domain page is displayed.
5. Click the **Authentication Policies** tab.
6. Click **Create Authentication Policy** and enter the following information:
   - **Name**: `OAAM Protected Resources`
   - **Description**: `Resources protected by OAAM`
   - **Authentication Scheme**: TAPScheme
7. Click **Apply**.
8. Repeat Steps 1 through 7, but enter the following values after clicking Create Authentication Policy:
   - **Name**: `LDAP Protected Resource`
   - **Description**: `Resources protected by LDAPScheme`
   - **Authentication Scheme**: LDAPScheme

17.12.5 Creating a Resource in Access Manager

Now that you have something to protect, you must create a resource in Access Manager and assign it to one of the policy groups you just created.

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Application Domains**.
3. Click **Search**.
4. Click **IAM Suite**.
5. Click the **Resources** tab.
6. Click **New Resource** and enter the following information:
   - **Type**: `http`
   - **Description**: `OAAM Test Page`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/oaam_sso.html`
   - **Protection Level**: `Protected`
   - **Authentication Policy**: `OAAM Protected Resources`
   - **Authorization Policy**: `Protected Resource Policy`
7. Click **Apply**.

Note: Unlike Oracle HTTP Server, displaying static HTML pages can be difficult. However, the purpose of creating this resource is to test OAAM.

17.12.6 Moving TAP Resource to LDAP Policy

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs," using the `oamadmin` account created previously.
2. Click on **Application Domains** under the **Access Manager** section.

   The Application Domains Search screen appears.

   Click **Search**.

   Click on **IAM** Suite to bring up the IAM Suite Domain page.

   Click on the **Authentication Policies** subtab.
3. Click **Protected Higher Level Policy**.
4. Click on the **Resources** subtab.
5. In the Resources window click **/oamTAPAuthenticate**.
6. Click **Delete**.
7. Click **Apply**.
8. Click on **Application Domains** under the **Access Manager** section.

   The Application Domains Search screen appears.

   Click **Search**.

   Click on **IAM** Suite to bring up the IAM Suite Domain page.

   Click on the **Authentication Policies** subtab.
9. Click **LDAP Protected Resources**.
10. In the Resources window, click **Add**.

    When the Search box appears enter:

    Resource URL: `/oamTAPAuthenticate`

    Click **Search**.

    Click on **/oamTAPAuthenticate** from the search results.

    Click **Add Selected**.
11. Click **Apply**.

17.12.7 Validating the Integration

Use the OAM Access Tester tool to ensure that this integration has been completed successfully.

To ensure the integration is completed successfully:

1. Ensure that *`JAVA_HOME`* is set in your environment.
2. Add *`JAVA_HOME`*`/bin` to your *`PATH`*, for example:

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

3. Change directory to:

   IAD_ORACLE_HOME/oam/server/tester

4. Start the test tool in a terminal window using the command:

   ```
   java -jar oamtest.jar
   ```

5. Connect using the following values:

   - **Primary OAM Host**: OAMHOST1
   - **Port**: 5575 (*OAM_PROXY_PORT*)
   - **Agent ID**: IAMSuiteAgent
   - **Agent Password**: Password you assigned to the IAMSuiteAgent profile
   - **Mode**: Select **List System Snapshots** for AIX platforms. Otherwise, select **Simple**.
   - **Global Passphrase**: If you selected Simple mode, enter the Access Manager global passphrase obtained in Section 17.12.1, "Retrieving the Global Passphrase for Simple Mode.".

   Click **Connect**.

6. Provide Protected Resource URI:

   - **Scheme**: http
   - **Host**: IAMSuiteAgent
   - **Port**: Leave blank
   - **Resource**: /oamTAPAuthenticate

   Click **Validate**.

7. Provide User Identity oamadmin and the password for oamadmin.

   Click **Authenticate**. If the authentication is successful, integration has been completed successfully.

Perform the same validation on OAMHOST2.

Access your protected resource using the following URL:

```
https://sso.mycompany.com:443/oaam_sso.html
```

You are redirected to OAAM for registration and challenge. The OAAM login page is shown instead of the Access Manager login page. Log in using an authorized Access Manager user such as oamadmin. Once you are logged in, the OAAM protected resource is displayed.

Note: Where Oracle Traffic Director is used, once you have been through the OAAM authentication, an error appears showing "page not found." This is expected, you have not created the `oaam_sso.html` page merely created a policy to test authentication.

If you have an Oracle HTTP Server, you can easily create a simple HTML page. This is possible in Oracle Traffic Director, but is complicated. If you are presented with an OAAM challenge when trying to access the resource, and you pass that validation, that is sufficient to validate OAAM. Whether or not a simple HTML page is displayed at the end is not relevant and does not invalidate the test.

17.13 Integrating Oracle Adaptive Access Manager 11*g* with Oracle Identity Manager 11*g*

OAAM provides a comprehensive set of challenge questions. Its functionality includes:

- Challenging the user before and after authentication, as required, with a series of questions.
- Presenting the questions as images and seeking answers through various input devices.
- Asking questions one after another, revealing subsequent questions only if correct answers are provided.

Oracle Identity Manager also has basic challenge question functionality. It enables users to answer a set of configurable questions and reset their password if they forgot the password. Unlike OAAM, Oracle Identity Manager also has a rich set of password validation capabilities, and it enables policies to be set based on the accounts owned, in addition to simple attributes.

In an Identity and Access Management deployment, best practice is to register only a single set of challenge questions, and to use a single set of password policies. OAAM can be integrated with Oracle Identity Manager so that OAAM provides the challenge questions and Oracle Identity Manager provides password validation, storage and propagation. This enables you to use OAAM fraud prevention at the same time you use Oracle Identity Manager for password validation. When OAAM is integrated with Oracle Identity Manager, Oracle Identity Manager is used to help users who have forgotten their username or password.

Note: Where Oracle Traffic Director is used, once you have been through the OAAM authentication, you see an error showing "page not found." This is expected, you have not created the `oaam_sso.html` page merely created a policy to test authentication.

If you have an Oracle HTTP Server server then creating a simple HTML page is easily done, and while possible in OTD it is complicated. So if you are presented with an OAAM challenge when trying to access the resource and you pass that validation that is sufficient to validate OAAM. Whether or not a simple HTML page is displayed at the end is not relevant, and does not invalidate the test.

This section contains the following topics:

- Section 17.13.1, "Configuring Oracle Identity Manager Encryption Keys in CSF"
- Section 17.13.2, "Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager"
- Section 17.13.3, "Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager"
- Section 17.13.4, "Setting Oracle Identity Manager Properties for OAAM"
- Section 17.13.5, "Restarting IAMAccessDomain and IAMGovernanceDomain"
- Section 17.13.6, "Validating Oracle Identity Manager-Oracle Adaptive Access Manager Integration"

17.13.1 Configuring Oracle Identity Manager Encryption Keys in CSF

1. Go to Oracle Enterprise Manager Fusion Middleware Control for the domain IAMAccessDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Log in using the WebLogic administrator account, for example `weblogic_idm`.
3. Expand the **WebLogic Domain** icon in the navigation tree in the left pane.
4. Select the IAMAccessDomain, right click, and select the menu option **Security** and then the option **Credentials** in the sub menu.
5. Click **oaam** to select the map and then click **Create Key**.
6. In the pop-up window, ensure **Select Map** is **oaam**.
7. Enter:
   - **Key Name**: `oim.credentials`
   - **Type**: `Password`
   - **UserName**: `xelsysadm`
   - **Password**: Password for `xelsysadm` account, *`COMMON_IDM_PASSWORD`*
8. Click **OK** to save the secret key to the Credential Store Framework.

17.13.2 Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

When you are deploying Oracle Adaptive Access Manager, and Oracle Identity Manager and Oracle Adaptive Access Manager are in separate domains, you must configure cross-domain trust.

Configure cross-domain trust in the domain IAMAccessDomain, as follows:

1. Log in to WebLogic Administration Console in IAMAccessDomain.
2. Click **Lock and Edit**.
3. Click **IAMAccessDomain** in **Domain Structure** and select the **Security** tab.
4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Choose a password to be used to confirm cross domain trust and type it in the **Credential and Confirm Credential** fields.
7. Click **Save**.

8. Click **Activate Changes**.

Configure Cross-Domain Trust in the domain IAMGovernanceDomain, as follows:

1. Log in to WebLogic Administration Console in IAMGovernanceDomain.
2. Click **Lock and Edit**.
3. Click **IAMGovernanceDomain** in **Domain Structure** and select the **Security** tab.
4. Expand the **Advanced** section.
5. Select **Cross domain security enabled**.
6. Enter the password you entered into the credential fields of the IAMAccessDomain in the **Credential and Confirm Credential** fields.
7. Click **Save**.
8. Click **Activate Changes**.

17.13.3 Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager

Go to the OAAM Administration Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."

Log in using the `oaamadmin` account you created in Section 17.3.2, "Creating OAAM Users and Groups in LDAP.""

Then proceed as follows:

1. In the navigation tree, click **Properties** under the **Environment** heading and then click **List Properties**. The properties search page is displayed.
2. To set a property value, enter its name in the **Name** field and click **Search**. The current value is shown in the search results window.
3. Click the entry. The **Value** field is displayed. Enter the new value and click **Save**.
4. Set the following properties to enable Oracle Adaptive Access Manager to integrate with Oracle Identity Manager:
   - **`bharosa.uio.default.user.management.provider.classname`**: `com.bharosa.vcrypt.services.OAAMUserMgmtOIM`
   - **`bharosa.uio.default.signon.links.enum.selfregistration.url`**: `https://sso.mycompany.com:443/identity/faces/register?&backUrl=https://sso.mycompany.com:443/identity`
   - **`bharosa.uio.default.signon.links.enum.trackregistration.enabled`**: `true`
   - **`bharosa.uio.default.signon.links.enum.selfregistration.enabled`**: `true`
   - **`bharosa.uio.default.signon.links.enum.trackregistration.url`**: `https://sso.mycompany.com:443/identity/faces/trackregistration?&backUrl=https://sso.mycompany.com:443/identity`
   - **`oaam.oim.passwordflow.unlockuser`**: `true`
   - **`oaam.oim.url`**: `t3://oimhost1vhn.mycompany.com:14000,oimhost2vhn.mycompany.com:14000`

17.13.4 Setting Oracle Identity Manager Properties for OAAM

1. Log in to the Oracle Identity Manager System Administration Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **System Configuration** under the **System Management** heading. The System Configuration window opens.
3. Click **Search** in **Search System Properties**.
4. Click each of the properties shown below, then select **Edit**. Set the value of each property as shown and click **Save** to save the value.

   Note: The property name appears in the **keyword** column.

   - `OIM.DisableChallengeQuestions`: `TRUE`
   - `OIM.ChangePasswordURL`: `https://sso.mycompany.com:443/oaam_server/oimChangePassword.jsp`
   - `OIM.ChallengeQuestionModificationURL`: `https://sso.mycompany.com:443/oaam_server/oimResetChallengeQuestions.jsp`

17.13.5 Restarting IAMAccessDomain and IAMGovernanceDomain

Restart the following Administration servers and managed servers as described in Chapter 20.1, "Starting and Stopping Components."

- WebLogic Administration Servers
- wls_oam1 and wls_oam2
- wls_oim1 and wls_oim2
- wls_oaam1 and wls_oaam2

17.13.6 Validating Oracle Identity Manager-Oracle Adaptive Access Manager Integration

Validate that Oracle Identity Manager is integrated with OAAM as follows:

Log in to the Oracle Identity Self Service as the `xelsysadm` user.

You are prompted to set up challenge questions and OAAM-specific security pictures.

17.14 Changing Domain to Oracle Adaptive Access Manager Protection

To use OAAM authentication for everything:

Note: Perform this procedure only if you want the entire domain to be protected by OAAM rather than just OAM.

---

1. Log in to the Access Management Console at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Application Domains**.
3. Click **Search**.

4. Click **IAM Suite**.
5. Click the **Authentication Policies** tab.
6. Click on the policy **Protected HigherLevel Policy**.
7. Change the value of **Authentication Scheme** to `TAPScheme`.
8. Click **Apply**.

17.15 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

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

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

1. Back up the web tier as described in Section 20.5.3.6, "Backing Up the Web Tier."
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Back up the Administration Server domain directory as described in Section 20.5.3.4, "Backing Up the WebLogic Domain IAMGovernanceDomain."
4. Back up the directory as described in Section 20.5.3.2, "Backing Up LDAP Directories."

For information about backing up the application tier configuration, see Section 20.5, "Performing Backups and Recoveries."

18 Configuring Server Migration for an Enterprise Deployment

Configuring server migration allows SOA-managed and Oracle Identity Manager-managed servers to be migrated from one host to another, so that if a node hosting one of the servers fails, the service can continue on another node. This chapter describes how to configure server migration for an Identity and Access Management enterprise deployment.

This chapter contains the following steps:

18.1 Overview of Server Migration for an Enterprise Deployment

Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers. The WLS_OIM1 and WLS_SOA1 Managed Server are configured to restart on OIMHOST2 should a failure occur. The WLS_OIM2 and WLS_SOA2 Managed Servers are configured to restart on OIMHOST1 should a failure occur. The WLS_OIM1, WLS_SOA1, WLS_OIM2 and WLS_SOA2 servers listen on specific floating IPs that are failed over by WebLogic Server Migration.

Perform the steps in the following sections configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers.

18.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

In this section, you set up a user and tablespace for the server migration leasing table:

> **Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi data source for database leasing do not need to be re-created, but they must be retargeted to the clusters being configured with server migration.

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the sysdba user and run the following command:

   ```
   create tablespace leasing
   logging datafile
   size 32m autoextend on;
   ```

   > **Note:** This is an example where Oracle Managed Files is configured. If you are not using Oracle Managed Files, refer to your database administrator guide for information about creating a tablespace.

2. Create a user named `leasing` and assign to it the `leasing` tablespace:

   ```
   create user leasing identified by password;
   grant create table to leasing;
   grant create session to leasing;
   alter user leasing default tablespace leasing;
   alter user leasing quota unlimited on leasing;
   ```

3. Create the `leasing` table using the `leasing.ddl` script:

   a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

   ```
   WL_HOME/server/db/oracle/817
   WL_HOME/server/db/oracle/920
   ```

   b. Connect to the database as the `leasing` user.

   c. Run the leasing.ddl script in SQL*Plus:

   ```
   @Copy_Location/leasing.ddl;
   ```

   d. Currently, the script does not commit the change. Enter the following, at the SQL*Plus prompt, after the tool completes:

   ```
   commit;
   ```

18.3 Creating a GridLink Data Source for Leasing Using the Oracle WebLogic Administration Console

In this section, you create a GridLink data source for the leasing table from the Oracle WebLogic Server Administration Console.

To create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.

3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
   - **Name**: Enter a logical name for the data source. For example, `leasing`.
   - **JNDI**: Enter a name for JNDI. For example, `jdbc/leasing`.
   - **Database Driver**: Select **For the Database Driver, select Oracle's Driver (Thin) for GridLink Connections Versions: 11 and later**.
   - Click **Next**.
5. In the Transaction Options page, de-select **Supports Global Transactions**, and click **Next**.
6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.
7. Enter the following connection properties:
   - **Service Name**: Enter the service name of the database (*`OIM_DB_SERVICENAME`*) with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example: `OIMEDG.mycompany.com`
   - **Host Name and Port**: Enter the SCAN address a
     nd port for the RAC database being used. You can identify this address by querying the appropriate parameter in the database using the TCP Protocol:

     ```
     show parameter remote_listener;

     NAME                 TYPE        VALUE

     -------------------------------------------------

     remote_listener     string      IAMDBSCAN.mycompany.com:1521
     ```

     Note:

   - **Database User Name**: leasing
   - **Password**: For example: welcome1
   - **Confirm Password**: Enter the password again and click **Next**.

     Leave the default setting for the remaining values.
8. On the Test GridLink Database Connection page, review the connection parameters and click **Test All Listeners**. Here is an example of a successful connection notification:

   ```
   Connection test for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
   LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN.mycompany.com)
   (PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=OIMEDG.mycompany.com))) succeeded.
   ```

   where port 1521 is *DB_LSNR_PORT* and `oimedg.mycompany.com` is *`OIM_DB_SERVICENAME`*.

   Click **Next**.
9. In the ONS Client Configuration page, do the following:
   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.

- Enter here also the SCAN address for the RAC database and the ONS remote port as reported by the database (example below) and click **ADD**:

  ```
  srvctl config nodeapps -s

  ONS exists: Local port 6100, remote port 6200, EM port 2016
  ```

- Click **Next**.

> **Note:** For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:
>
> ```
> IAMDBHOST1.mycompany.com (port 6200)
> ```
>
> and
>
> ```
> IAMDBHOST2.mycompany.com (port 6200)
> ```

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for IAMDBSCAN.mycompany.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select **oim_cluster** and **soa_cluster** as the targets, and **All Servers in the cluster**.
12. Click **Finish**.
13. Click **Activate Changes**.

18.4 Editing Node Manager's Properties File

In this section, you edit Node Manager's properties file. This must be done for the Node Managers on the nodes where the servers are running, OIMHOST1 and OIMHOST2.

The `nodemanager.properties` file is located in the following directory:

```
SHARED_CONFIG_DIR/nodemanager
```

Add the following properties to enable server migration to work properly:

- `Interface:`

  ```
  Interface=bond0
  ```

  This property specifies the interface name for the floating IP. This will be `bond0` in most topologies. If external Oracle HTTP servers are being used, the managed servers will be listening on `bond1`. In that case, the `bond1` interface must be used here.

- `NetMask:`

  ```
  NetMask=255.255.254.0
  ```

  This property specifies the net mask for the interface for the floating IP. The net mask should the same as the net mask on the interface.

- UseMACBroadcast:

  ```
  UseMACBroadcast=true
  ```

  This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the -b flag in the arping command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
StateCheckInterval=500
bond0=*,NetMask=255.255.254.0
UseMACBroadcast=true
```

> **Note:** The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. If not done already, set the StartScriptEnabled property in the nodemanager.properties file to true. This is required to enable Node Manager to start the managed servers.
2. Start Node Manager on OIMHOST1 and OIMHOST2 by running the startNodeManager.sh script, which is located in the *WL_HOME*/server/bin directory, or use the procedure described in Section 20.1.3.5.1, "Starting Node Manager."

18.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

On Linux, you set environment and superuser privileges for the wlsifconfig.sh script:

Ensure that your PATH environment variable includes the files listed in Table 18–1.

Table 18–1 Files Required for the PATH Environment Variable

File	Located in this directory
wlsifconfig.sh	*IGD_MSERVER_HOME*/bin/server_migration
wlscontrol.sh	*WL_HOME*/common/bin
nodemanager.domains	*WL_HOME*/common/nodemanager

Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.

For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform the following steps to set the environment and superuser privileges for the wlsifconfig.sh script.

> **Note:** Ask the system administrator for the appropriate sudo and system rights to perform this step.

Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside `/etc/sudoers` granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`.

To grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

18.6 Configuring Server Migration Targets

In this section, you configure server migration targets. Configuring Cluster Migration sets the `DataSourceForAutomaticMigration` property to `true`.

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console in the IAMGovernanceDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (**oim_cluster**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock and Edit**.
6. In the **Available** field, select the machines to which to allow migration, **OIMHOST1** and **OIMHOST2**, and click the right arrow.
7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
10. Select the server for which you want to configure migration.
11. Click the **Migration** tab.
12. Select **Automatic Server Migration Enabled** and click **Save**.
13. Click **Activate Changes**.
14. Repeat steps 2 through 13 for the SOA cluster.
15. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured, as described in Section 20.1, "Starting and Stopping Components."

18.7 Testing the Server Migration

In this section, you test that server migration is working properly.

The best way to validate server migration is to start Node Manager manually in a console window as described in Section 20.1.3.5.1, "Starting Node Manager."

To test from OIMHOST1:

1. Stop the WLS_OIM1 Managed Server. To do this, run this command:

   ```
   kill -9 pid
   ```

   where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

   ```
   ps -ef | grep WLS_OIM1
   ```

2. Watch the Node Manager terminal. You should see a message indicating that WLS_OIM1's floating IP has been disabled.
3. Wait for Node Manager to try a second restart of WLS_OIM1. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

To test from OIMHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart WLS_OIM1 on OIMHOST1, Node Manager on OIMHOST2 should prompt that the floating IP for WLS_OIM1 is being brought up and that the server is being restarted in this node.
2. Access the Oracle Identity Manager Console using the Virtual Host Name, for example: `http://OIMHOST1VHN.mycompany.com:14000/identity`.

Follow the previous steps to test server migration for the WLS_OIM2, WLS_SOA1, and WLS_SOA2 Managed Servers.

Table 18–2 shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 18–2 Managed Server Migration

Managed Server	Migrated From	Migrated To
WLS_OIM1	OIMHOST1	OIMHOST2
WLS_OIM2	OIMHOST2	OIMHOST1
WLS_SOA1	OIMHOST1	OIMHOST2
WLS_SOA2	OIMHOST2	OIMHOST1

Verification From the WebLogic Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain at the address listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **IAMGovernanceDomain** on the left pane.
3. Click the **Monitoring** tab and then the **Migration** sub tab.

   The Migration Status table provides information on the status of the migration.

Note: After a server is migrated, to fail it back to its original node/machine, stop the migrated Managed Server from the Oracle WebLogic Administration Console and see that the appropriate Node Manager starts the original Managed Server on the originally assigned machine.

18.8 Backing Up the Server Migration Configuration

Back up the database and the WebLogic domain, as described in Section 20.5.3, "Performing Backups During Installation and Configuration."

19 Scaling Enterprise Deployments

The reference enterprise topology discussed in this guide is highly scalable. It can be scaled up and or scaled out. This chapter explains how to do so.

To scale up the topology, you add a new component instance to a node already running one or more component instances. To scale out the topology, you add new component instances to new nodes.

This chapter contains the following topics:

19.1 Scaling the Topology

The Oracle Identity and Access Management topology described in the guide has three tiers: the Directory Tier, Application Tier and Web Tier. The components in all three tiers of the Oracle Identity and Access Management topology described in this guide can be scaled up or scaled out.

In this release, the Identity and Access Management Deployment tool cannot be used to scale out or scale up components. Scaling up or out is a manual process, as described in this chapter.

You scale up a topology by adding a new server instance to a node that already has one or more server instances running. You scale out a topology by adding new components to new nodes.

19.2 Scaling the LDAP Directory

Scale the LDAP Directory as follows.

19.2.1 Mounting the Middleware Home when Scaling Out

Oracle Binaries are shared among the LDAP hosts. When scaling out, you must mount the shared binary directory onto the new host.To do this, perform the steps in Section 9.10, "Mounting Shared Storage onto the Host."

19.2.2 Scaling Oracle Unified Directory

The binaries for Oracle Unified Directory are located in *IDM_TOP*, which is shared among the LDAPHOSTs. When scaling out Oracle Unified Directory to a new host, ensure that this directory is mounted to the new host. See Section 9.10, "Mounting Shared Storage onto the Host."

The directory tier has two Oracle Unified Directory nodes, LDAPHOST1 and LDAPHOST2, each running an Oracle Unified Directory instance. The Oracle Unified Directory binaries on either node can be used for creating the new Oracle Unified Directory instance.

Proceed as follows:

1. Assemble information, as listed in Section 19.2.2.1, "Assembling Information for Scaling Oracle Unified Directory."
2. If scaling out, mount the shared storage onto the new LDAPHOST.
3. Follow the steps in Section 19.2.2.2, "Configuring an Additional Oracle Unified Directory Instance."
4. Follow the steps in Section 19.2.2.3, "Validating the New Oracle Unified Directory Instance."
5. Follow the steps in Section 19.2.2.4, "Adding the New Oracle Unified Directory Instance to the Load Balancers."
6. Reconfigure the load balancer with the host and port information of the new Oracle Unified Directory instance, as described in Section 19.4.5, "Reconfiguring the Load Balancer."

19.2.2.1 Assembling Information for Scaling Oracle Unified Directory

Assemble the following information before scaling Oracle Unified Directory.

Description	Variable	Documented Value	Customer Value
New Oracle Unified Directory Host Name	*LDAP_HOST*	LDAPHOST3.mycompany.com	
Oracle Unified Directory Listen Port	*LDAP_PORT*	1389	
Oracle Unified Directory SSL Port	*LDAP_SSL_PORT*	1636	
Oracle Unified Directory Administration Port	*LDAP_ADMIN_PORT*	4444	
Oracle Unified Directory Replication Port	*LDAP_REPLIC_PORT*	8989	
Oracle Instance Location	*OUD_ORACLE_INSTANCE*	`/u02/private/oracle/config/instances/oudn`	
Oracle Unified Directory Existing Instance/Component Name	oud*n*	oud1	
Newly Created Instance/Component Name	oud*n*	oud3	
Oracle Unified Directory Administrator Password	*COMMON_IDM_PASSWORD*		
Common Password	*COMMON_IDM_PASSWORD*		

19.2.2.2 Configuring an Additional Oracle Unified Directory Instance

If you are scaling out to another machine, you can use ports 1389 (*LDAP_PORT*), 1636 *(LDAP_SSL_PORT*), 4444 (*LDAP_ADMIN_PORT*), and 8989 (*LDAP_REPLIC_PORT*). If you are scaling up, those ports are already in use and you must choose unique ports. Ensure that the ports you plan to use are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

```
netstat -an | grep "1389"
```

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

Remove the entries for the ports you freed from the `/etc/services` file and restart the services or restart the computer.

Set the environment variable `JAVA_HOME`

Set the environment variable `INSTANCE_NAME` to a new instance value, such as: `../../../../u02/private/oracle/config/instances/oud3`

Note the tool creates the instance home relative to the *`OUD_ORACLE_HOME`*, so you must include previous directories to get the instance created in *`OUD_ORACLE_INSTANCE`*.

Change Directory to *`OUD_ORACLE_HOME`*

Start the Oracle Unified Directory configuration assistant by executing the command:

```
./oud-setup
```

1. On the Welcome screen, click **Next**.
2. On the Server Settings screen, enter:
   - **Host Name**: The name of the host where Oracle Unified Directory is running, for example: LDAPHOST3
   - **LDAP Listener Port**: 1389 (*LDAP_PORT*) if scaling out, unique port if scaling up.
   - **Administration Connector Port**: 4444 (*LDAP_ADMIN_PORT*)
   - LDAP Secure Access
     - Click **Configure**
     - Select **SSL Access**
     - **Enable SSL on Port**: 1636 *(LDAP_SSL_PORT*)
     - **Certificate**: Generate Self Signed Certificate OR provide details of your own certificate.
     - Click **OK**
   - **Root User DN**: Enter an administrative user for example `cn=oudadmin`
   - **Password**: Enter the password you want to assign to the ouadmin user. Using the *`COMMON_IDM_PASSWORD`* is recommended.
   - **Password (Confirm)**: Repeat the password.
   - Click **Next**.
3. On the Topology Options screen, enter
   - **This server will be part of a replication topology**

- **Replication Port:** (*`LDAP_REPLIC_PORT`*) 8989
- Select **Configure As Secure,** if you want replication traffic to be encrypted.
- **There is already a server in the topology**: Selected.

  Enter the following:

  – **Host Name**: The name of the Oracle Unified Directory server host for this instance, for example: LDAPHOST1.mycompany.com

  – **Administrator Connector Port**: 4444 (*LDAP_ADMIN_PORT*)

  – **Admin User**: Name of the Oracle Unified Directory administrative user on LDAPHOST1, for example: `cn=oudadmin`

  – **Admin Password**: Administrator password. Using the *`COMMON_IDM_PASSWORD`* is recommended.

  Click **Next**.

  If you see a certificate Not Trusted Dialogue, it is because you are using self signed certificates. Click **Accept Permanently.**

Click **Next**.

4. On The Create Global Administrator Screen Enter:

   - **Global Administrator ID:** The name of an account you want to use for managing Oracle Unified Directory replication, for example: `oudmanager`
   - **Global Administrator Password / Confirmation**: Enter a password for this account. Using the *`COMMON_IDM_PASSWORD`* is recommended.

   Click **Next**.

5. On the Data Replication Screen. select `dc=mycompany,dc=com` and click **Next**.
6. On the Oracle Components Integration screen, click **Next**.
7. On the Runtime Options Screen Click Next.
8. On the Review Screen, check that the information displayed is correct and click **Finish**.
9. On the Finished screen, click **Close**.

19.2.2.3 Validating the New Oracle Unified Directory Instance

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

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapsearch -h LDAPHOST3.mycompany.com -p 1389 -D
cn=oudadmin -b "" -s base "(objectclass=*)" supportedControl
```

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

19.2.2.4 Adding the New Oracle Unified Directory Instance to the Load Balancers

Add the new Oracle Unified Directory instance to the existing server pool defined on the load balancer for distributing requests across the instances.

19.3 Scaling Identity and Access Management Applications

The Application Tier has two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Access Management Access Manager, and two nodes (OIMHOST1 and OIMHOST2) running Managed Servers for Oracle Identity Manager. Optionally, the Application Tier might have two nodes (OAMHOST1 and OAMHOST2) running Managed Servers for Oracle Adaptive Access Manager.

This section contains the following topics:

- Section 19.3.1, "Gathering Information."
- Section 19.3.2, "Mounting Middleware Home and Creating a New Machine when Scaling Out."
- Section 19.3.3, "Creating a New Node Manager when Scaling Out."
- Section 19.3.4, "Running Pack/Unpack."
- Section 19.3.5, "Performing Application-Specific Steps."
- Section 19.3.6, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files."

19.3.1 Gathering Information

Use the following tables to assemble the values you need.

19.3.1.1 Assembling Information for Scaling Access Manager

Assemble the following information before scaling Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	NEWHOST*n*		
Existing Access Manager server		WLS_OAM1	
New Access Manager server name	WLS_OAM*n*	WLS_OAM3	
Server Listen Port	*OAM_PORT*	14100	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IADADMINVHN.mycompany.com	
WebLogic Administration Port	*IAD_WLS_PORT*	7001	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

19.3.1.2 Assembling Information for Scaling Oracle Identity Manager

Description	Variable	Documented Value	Customer Value
Host name	NEWHOST*n*		
SOA virtual server name		SOAHOST*x*VHN	
Oracle Identity Manager virtual server name		OIMHOST*x*VHN	
Existing SOA managed server to clone	WLS_SOA*n*	WLS_SOA1	

Description	Variable	Documented Value	Customer Value
Existing Oracle Identity Manager managed server to clone	`WLS_OIMn`	`WLS_OIM1`	
New SOA managed server name	`WLS_SOAn`	`WLS_SOA3`	
New Oracle Identity Manager managed server name	`WLS_OIMn`	`WLS_OIM3`	
Numeric extension for new JMS servers	*n*	3	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IGDADMINVHN.mycompany.com	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7101	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

19.3.1.3 Assembling Information for Scaling Oracle Adaptive Access Manager

Assemble the following information before scaling Oracle Adaptive Access Manager.

Description	Variable	Documented Value	Customer Value
Host Name	*NEWHOSTn*		
Existing OAAM server		`WLS_OAAM1`	
New OAAM server name	*WLS_OAAMn*	`WLS_OAAM3`	
Server Listen Address			
OAAM Managed Server Port	*OAAM_PORT*	14300	
OAAM Administration Managed Server Port	*OAAM_ADMIN_PORT*	14200	
WebLogic Administration Host	*WLS_ADMIN_HOST*	IDADMINVHN.mycompany.com[1]	
WebLogic Administration Port	*WLS_ADMIN_PORT*	7001	
WebLogic Administration User		weblogic_idm	
WebLogic Administration Password			

[1] This refers to the domain that you are scaling.

19.3.2 Mounting Middleware Home and Creating a New Machine when Scaling Out

Before scaling out a component of the OAM application tier, mount the Middleware home and create a new machine.

To mount the Middleware home and create a new machine:

1. On the new node, mount the existing Middleware home, which should include the Oracle Fusion Middleware installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain. See Section 9.10, "Mounting Shared Storage onto the Host." for more information.
2. To attach *IAD_ORACLE_HOME* in shared storage to the local Oracle Inventory, execute the following command:

```
cd IAD_ORACLE_HOME/oui/bin
./attachHome.sh -jreLoc JAVA_HOME
```

> **Note:** This section uses IAD_ORACLE_HOME as an example. Use the same procedure for IGD_ORACLE_HOME.

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `HOME/bea/beahomelist` file and add `IAD_MW_HOME/oui/bin` to it.
4. Log in to the WebLogic Administration Console for the IAMAccessDomain at the address listed in Section 20.2, "About Identity and Access Management Console URLs."
5. Create a new machine for the new node to be used, and add the machine to the domain, as follows.
   a. Select **Environment -> Machines** from the Navigation menu.
   b. Click **Lock and Edit**.
   c. Click **New** on the Machine Summary screen.
   d. Enter the following information:

      Name: Name of the machine (NEWHOSTn)

      Machine OS: Select UNIX.
   e. Click **Next**.
   f. On the Node Manager Properties page, enter the following information:

      Type: SSL.

      Listen Address: *NEWHOSTn*.
   g. Click **Finish**.
   h. Click **Activate Changes**.

19.3.3 Creating a New Node Manager when Scaling Out

Node Manager is used to start and stop WebLogic managed servers on the new host. In order to create a new node manager for the new host perform the following steps:

1. Create a new directory for the new node manager by copying an existing one. Copy the directory `SHARED_CONFIG/nodemanager/oamhost1.mycompany.com` to: `SHARED_CONFIG/nodemanager/newiamhost.mycompany.com`

   For example:

   ```
   cp -r $SHARED_CONFIG/nodemanager/oamhost1.mycompany.com $SHARED_
   CONFIG/nodemanager/newiamhost.mycompany.com
   ```

2. Change to the newly created directory.

   ```
   cd SHARED_CONFIG/nodemanager/NEWHOST3.mycompany.com
   ```

3. Edit the `nodemanager.properties` file, changing all the entries for OAMHOST1 to `OAMHOST3`. For example:

   ```
   DomainsFile=/u01/oracle/config/nodemanager/OAMHOST1.mycompany.com/nodemanager.d
   ```

```
omain
```

becomes

```
DomainsFile=/u01/oracle/config/nodemanager/NEWHOST3.mycompany.com/nodemanager.d
omain
```

4. Edit the `startNodeManagerWrapper.sh` file, changing all the entries for OAMHOST1 to OAMHOST3. For example:

   ```
   NM_HOME=/u01/oracle/config/nodemanager/oamhost1.mycompany.com
   ```

   becomes

   ```
   NM_HOME=/u01/oracle/config/nodemanager/oamhost3.mycompany.com
   ```

5. Start the node manager by invoking the command:

   ```
   ./startNodeManagerWrapper.sh
   ```

6. Update the node manager configuration by following the steps in Chapter 19.5.4, "Updating Node Manager Configuration" to ensure that certificates are created for the new host.

19.3.4 Running Pack/Unpack

Whenever you extend a domain to include a new managed server, you must extract the domain configuration needs from the *ASERVER_HOME* location to the *MSERVER_HOME* location. This applies whether you are scaling up or out. To do this perform the following steps.

> **Note:** The following steps are an example of packing and unpacking the IAMAccessDomain

1. Pack the domain on the host where the administration server is located, for example: OAMHOST1:

   ```
   pack.sh -domain=IAD_ASERVER_HOME -template =/templates/managedServer.jar
   -template_name="template_name" -managed=true
   ```

   The `pack.sh` script is located in *ORACLE_COMMON_HOME*`/common/bin`.

2. Unpack the domain on the new host for scale out, or on the existing host for scale up, using the command:

   ```
   unpack.sh -domain=IAD_MSERVER_HOME -template=/templates/managedServer.jar -app_
   dir=IAD_MSERVER_HOME/applications
   ```

   The `unpack.sh` script is located in *ORACLE_COMMON_HOME*`/common/bin`.

3. If you are scaling out, start Node Manager and update the property file.

   a. Start and stop Node Manager as described in Section 20.1, "Starting and Stopping Components."

   b. Run the script `setNMProps.sh`, which is located in *ORACLE_COMMON_HOME*`/common/bin`, to update the node manager properties file, for example:

      ```
      cd ORACLE_COMMON_HOME/common/bin
      ./setNMProps.sh
      ```

c. Start Node Manager once again as described in Section 20.1, "Starting and Stopping Components."

19.3.5 Performing Application-Specific Steps

This section contains the following topics:

- Section 19.3.5.1, "Clone an Existing Managed Server."
- Section 19.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 19.3.5.2, "Scaling Oracle Access Management Access Manager."
- Section 19.3.5.3, "Scaling Oracle Identity Manager"
- Section 19.3.5.4, "Updating Oracle Adaptive Access Manager Integration"

19.3.5.1 Clone an Existing Managed Server

Create a new managed server by cloning an existing managed server of the same type. To scale out/up Access Manager, clone `wls_oam1`. Similarly, to scale out/up Identity Manager, clone `wls_oim1`.

The following example is for cloning an Access Manager managed server, although the procedure is the same for all products.

1. Log in to the Oracle WebLogic Administration Console for the domain whose managed server you are cloning, at the address listed in Section 20.2, "About Identity and Access Management Console URLs." For this example the domain is `IAMAccessDomain`.
2. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
3. Click **Lock & Edit** from the Change Center menu.
4. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.
5. Click **Clone**.
6. Enter the following information:
   - **Server Name**: A new name for the server, for example: `WLS_OAM3`.
   - **Server Listen Address**: The name of the host on which the Managed Server runs.
   - **Server Listen Port**: The port the new Managed Server uses. This port must be unique within the host.

     If you are scaling out, you can use the default port, `14100` (*`OAM_PORT`* in Table 7–1). If you are scaling up, choose a unique port.
7. Click **OK**.
8. Click the newly created server **WLS_OAM3**
9. Set **Machine** to be the machine you created in Section 19.3.2, "Mounting Middleware Home and Creating a New Machine when Scaling Out""
10. Click **Save**.
11. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_OAM3` Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the

communication between the Oracle WebLogic Administration Server and the Node Manager in `NEWHOST`.

If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings were propagated to the cloned server. To disable host name verification:

a. In Oracle Enterprise Manager Fusion Middleware Control, select **Oracle WebLogic Server Administration Console**.

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

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

d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.

e. Click the **SSL** tab.

f. Click **Advanced**.

g. Set **Hostname Verification** to `None`.

h. Click **Save**.

12. Click **Activate Changes** from the Change Center menu.

19.3.5.2 Scaling Oracle Access Management Access Manager

This section contains steps specific to scaling Access Manager.

> **Note:** If you are using shared storage, allow the new host access to that shared storage area.

Scale Oracle Access Management Access Manager by performing the steps in the following subsections:

- Section 19.3.5.2.1, "Run Pack/Unpack"
- Section 19.3.5.2.2, "Register Managed Server with Oracle Access Management Access Manager"
- Section 19.3.5.2.3, "Update WebGate Profiles"
- Section 19.3.5.2.4, "Update the Web Tier"

19.3.5.2.1 Run Pack/Unpack Run `pack` and `unpack` as described in Section 15.3.4, "Running Pack/Unpack."

19.3.5.2.2 Register Managed Server with Oracle Access Management Access Manager Register the new Managed Server with Oracle Access Management Access Manager. You now must configure the new Managed Server now as an Access Manager server. You do this from the Oracle Access Management Console. Proceed as follows:

1. Log in to the Access Management console at `http://IADADMIN.mycompany.com/oamconsole` as the user identified by the entry in Section 13.9, "Set User Names and Passwords"
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.

5. Enter the following information:
   - **Server Name**: `WLS_OAM3`
   - **Host**: Host that the server runs on
   - **Port**: Listen port that was assigned when the Managed Server was created
   - **OAM Proxy Port**: Port you want the Access Manager proxy to run on. This is unique for the host
   - **Proxy Server ID**: `AccessServerConfigProxy`
   - **Mode**: Set to same mode as existing Access Manager servers.
6. Click **Coherence** tab.

   Set **Local Port** to a unique value on the host.
7. Click **Apply**.
8. Restart the WebLogic Administration Server as described in Section 20.1, "Starting and Stopping Components"

19.3.5.2.3 Update WebGate Profiles Add the newly created Access Manager server to all WebGate Profiles that might be using it, such as `Webgate_IDM`, `Webgate_IDM_11g`, and `IAMSuiteAgent`

For example, to add the Access Manager server to `Webgate_IDM`, access the Access Management console at: `http://IADADMIN.mycompany.com/oamconsole`

Then proceed as follows:

1. Log in as the Access Manager Administrative User.
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings** - **SSO Agents** - **OAM Agents**.
4. Click the open folder icon, then click **Search**.

   You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.
7. Click **+** in the **Primary Server** list (or the **Secondary Server** list if this is a secondary server).
8. Select the newly created managed server from the **Server** list.
9. Set **Maximum Number of Connections** to `10`.
10. Click **Apply**.

Repeat Steps 5 through 10 for **Webgate_IDM_11g**, **IAMSuiteAgent**, and all other WebGates that might be in use.

You can now start the new Managed Server, as described in Section 20.1, "Starting and Stopping Components"

19.3.5.2.4 Update the Web Tier Add the newly added Managed Server host name and port to the list WebLogicCluster parameter, as described in Section 19.3.6, "Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files"

Save the file and restart the Oracle HTTP server, as described in Section 20.1, "Starting and Stopping Components"

19.3.5.3 Scaling Oracle Identity Manager

You already have a node that runs a Managed Server configured with Oracle SOA Suite and Oracle Identity Manager components. The node contains a Middleware home, a SOA Oracle home, an Oracle Identity Manager Oracle home, and a domain directory for existing Managed Servers. Use the existing installations in shared storage for creating a new WLS_SOA and WLS_OIM managed server. There is no need to install the Oracle Identity and Access Management or Oracle SOA Suite binaries in a new location

When scaling up, you add WLS_SOA and WLS_OIM managed servers to existing nodes.

In either case, you must run pack and unpack.

When you scale out the topology, you add new Managed Servers configured with Oracle Identity Manager and SOA to new nodes. First check that the new node can access the existing home directories for WebLogic Server, Oracle Identity Manager, and SOA. You do need to run pack and unpack to bootstrap the domain configuration in the new node.

Follow the steps in the following subsections to scale the topology:

- Section 19.3.5.3.1, "Configuring New JMS Servers"
- Section 19.3.5.3.2, "Performing Pack/Unpack When Scaling Out"
- Section 19.3.5.3.3, "Specifying the Host Name Used by Oracle Coherence"
- Section 19.3.5.3.4, "Completing the Oracle Identity Manager Configuration Steps"

19.3.5.3.1 Configuring New JMS Servers Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server. You do this as follows:

1. Log in to the WebLogic Administration Server in the IAMGovernanceDomain, as described in Section 20.2, "About Identity and Access Management Console URLs," and navigate to **Services -> Messaging -> JMS Servers**.
2. Click **New**.
3. Enter a value for **Name**, such as `BPMJMSServer_auto_3`.
4. Click **Create New Store**.
5. Select `FileStore` from the list
6. Click **Next**.
7. Enter a value for **Name**, such as `BPMJMSFileStore_auto_3`
8. Enter the following values:

   Target: The new server you are creating.

   Directory: *`IGD_ASERVER_HOME`*`/jms/BPMJMSFileStore_auto_3`
9. Click **OK**.
10. When you are returned to the JMS Server screen, select the newly created file store from the list.
11. Click **Next**.
12. On the next screen set the Target to the server you are creating.
13. Click **Finish**.

Create the following JMS Queues depending on the managed server you are creating:

Server	JMS Server Name	File Store Name	Directory	Target
WLS_SOA*n*	BPMJMSServer_auto_*n*	BPMJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/BPMJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	SOAJMSServer_auto_*n*	SOAJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/SOAJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_SOA*n*	UMSJMSServer_auto_*n*	UMSJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/UMSJMSFileStore_auto_`*n*	WLS_SOA*n*
WLS_OIM*n*	JRFWSAsyncJmsServer_auto_*n*	JRFWSAsyncFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/RFWSAsyncFileStore_auto_`*n*	WLS_OIM*n*
WLS_OIM*n*	OIMJMSServer_auto_*n*	OIMJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/OIMJMSFileStore_auto_`*n*	wls_OIM*n*
WLS_SOA*n*	PS6SOAJMSServer_auto_*n*	PS6SOAJMSFileStore_auto_*n*	*IGD_ASERVER_HOME*`/jms/PS6SOAJMSFileStore_auto_`*n*	wls_SOA*n*

Add the newly created JMS Queues to the existing JMS Modules by performing the following steps:

1. Log in to the WebLogic Administration Console in the IAMGovernanceDomain, at the address listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Navigate to **Services -> Messaging -> JMS Modules**
3. Click a JMSModule, such as **SOAJMSModule**
4. Click the **Sub Deployments** tab.
5. Click the listed sub deployment.

> **Note:** This subdeployment module name is a random name in the form of **JMSServerName*XXXXXX*** resulting from the Configuration Wizard JMS configuration.

6. Assign the newly created JMS server, for example **SOAJMSServer_auto*n***.
7. Click **Save**.
8. Perform this for each of the JMS modules listed in the following table:

JMS Module	JMS Server
BPMJMSModule	BPMJMSServer_auto_*n*
JRFWSAsyncJmsModule	JRFWSAsyncJmServer_auto_*n*
OIMJMSModule	OIMJMSServer_auto_*n*
SOAJMSModule	SOAJMSServer_auto_*n*
UMSJMSSystemResource	UMSJMSServe_auto_*n*

9. Click **Activate Configuration** from the Change Center menu.

19.3.5.3.2 Performing Pack/Unpack When Scaling Out This section is necessary only when you are scaling out.

Run `pack` and `unpack` as described in Section 19.3.4, "Running Pack/Unpack"

19.3.5.3.3 Specifying the Host Name Used by Oracle Coherence Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

> **Note:** An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

Specify the nodes using the `tangosol.coherence.wka`*`n`* system property, where *`n`* is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses, for example: SOAHOST3VHN. Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab. You will also need to add the new server to the existing entries.

> **Tip:** To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

> **Note:** SOAHOST3VHN is the virtual host name that maps to the virtual IP where WLS_SOA3 listening (in SOAHOST3).

To add the host name used by Oracle Coherence:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (**WLS_SOA1** or **WLS_SOA2**, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit**.

6. Click the **Server Start** tab.
7. Enter the following for WLS_SOA1, WLS_SOA2, and WLS_SOA3 into the Arguments field.

   For WLS_SOA1, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST1VHN
   ```

   For WLS_SOA2, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST2VHN
   ```

   For WLS_SOA3, enter the following:

   ```
   -Dtangosol.coherence.wka1=SOAHOST1VHN
   -Dtangosol.coherence.wka2=SOAHOST2VHN
   -Dtangosol.coherence.wka3=SOAHOST3VHN
   -Dtangosol.coherence.localhost=SOAHOST3VHN
   ```

   > **Note:** There should be no breaks in lines between the different `-D` parameters. Do not copy or paste the text to your Administration Console's arguments text field. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST1VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST2VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

WLS_SOA3 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN
-Dtangosol.coherence.wka2=SOAHOST2VHN
-Dtangosol.coherence.wka3=SOAHOST3VHN
-Dtangosol.coherence.localhost=SOAHOST3VHN
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.wka3.port=8089
```

For more information about Coherence Clusters see the *Oracle Coherence Developer's Guide*.

8. Click **Save** and **Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

> **Note:** The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

19.3.5.3.4 Completing the Oracle Identity Manager Configuration Steps

1. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

   From the WebLogic Administration Console, select the **Server_name** > **Configuration** > **Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

2. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOA`*`n`* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `OIMHOST`*`n`*. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

   To disable host name verification:

   a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.

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

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

   d. Select **WLS_SOA*n*** in the Names column of the table. The Settings page for the server appears.

   e. Click the **SSL** tab.

   f. Click **Advanced**.

   g. Set **Hostname Verification** to `None`.

   h. Click **Save**.

3. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIM`*`n`* Managed Servers. In Step d, select **WLS_OIM*n*** in the Names column of the table.

4. Click **Activate Changes** from the Change Center menu.

5. Restart the WebLogic Administration Server as described in Section 20.1, "Starting and Stopping Components"

6. Start and test the new Managed Server from the Administration Console.

   a. Shut down the existing Managed Servers in the cluster.

   b. Ensure that the newly created Managed Server, `WLS_SOA`*`n`*, is up.

   c. Access the application on the newly created Managed Server (`http://vip:port/soa-infra`). The application should be functional.

7. Configure the newly created managed server for server migration. Follow the steps in Section 18.6, "Configuring Server Migration Targets"to configure server migration.

> **Note:** Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP addresses for the new Managed Servers are already present in the new node.

8. Test server migration for this new server. Follow these steps from the node where you added the new server:

   a. Stop the `WLS_SOA`*n* Managed Server.

      To do this, run:

      ```
      kill -9 pid
      ```

      on the process ID (PID) of the Managed Server. You can identify the PID of the node using

      ```
       ps -ef | grep WLS_SOAn
      ```

   b. Watch the Node Manager Console. You should see a message indicating that the floating IP address for WLS_SOA1 has been disabled.

   c. Wait for the Node Manager to try a second restart of WLS_SOA*n*. Node Manager waits for a fence period of 30 seconds before trying this restart.

   d. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.

   e. Repeat Steps a-d for WLS_OIM*n*.

19.3.5.4 Updating Oracle Adaptive Access Manager Integration

If you have extended your domain with Oracle Adaptive Access Manager and have integrated Oracle Identity Manager with Oracle Adaptive Access Manager, you must update Oracle Adaptive Access Manager so that it is aware of the new Oracle Identity Manager server. See Section 17.13.3, "Setting Oracle Adaptive Access Manager Properties for Oracle Identity Manager" for details.

19.3.6 Adding New WebLogic Managed Server to Oracle HTTP Server Configuration Files

Scaling an Application Tier component typically requires you to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

In the Web tier, there are several configuration files under *`WEB_ORACLE_INSTANCE`*`/config/OHS/componentname/moduleconf`, including `admin_vh.conf`, `sso_vh.conf` and `idminternal_vh.conf`. Each contain a number of entries in location blocks. If a block references two server instances and you add a third one, you must update that block with the new server.

For example if you add a new Access Manager server, you must update `sso_vh.conf` to include the new managed server. You add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100,OAMHOST1.mycompany.com:1
4101
</Location>

<Location /oamfed>
   SetHandler weblogic-handler
   WebLogicCluster
OAMHOST1.mycompany.com:14100,OAMHOST2.mycompany.com:14100,OAMHOST3.mycompany.com:1
4100
</Location>
```

Once you have updated the configuration file, restart the Oracle HTTP server(s) as described in Section 20.1, "Starting and Stopping Components." Oracle recommends that you do this sequentially to prevent loss of service.

19.4 Scaling the Web Tier

The Web Tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance.

To scale the Oracle HTTP Server, perform the steps in the following subsections:

- Section 19.4.1, "Assembling Information for Scaling the Web Tier."
- Section 19.4.2, "Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out."
- Section 19.4.3, "Running the Configuration Wizard to Configure the HTTP Server."
- Section 19.4.4, "Registering Oracle HTTP Server with WebLogic Server."
- Section 19.4.5, "Reconfiguring the Load Balancer."
- Section 19.4.6, "Scaling Up Oracle Traffic Director."

19.4.1 Assembling Information for Scaling the Web Tier

Assemble the following information before scaling the Web Tier.

Description	Variable	Documented Value	Customer Value
Host name		WEBHOST1.mycompany.com	
OHS port	*WEB_HTTP_PORT*	7777	
Instance Name	web*n*	web1 or web2	

Description	Variable	Documented Value	Customer Value
Component Name	web*n*	web1 or web2	
WebLogic Administration Host, IAMAccessDomain	*IADADMINVHN*	IADADMINVHN.mycompany.com	
Access Management WLS Server Port	*IAD_WLS_PORT*	7001	
WebLogic Administrative User		weblogic_idm	
WebLogic Administrative Password			

19.4.2 Mounting Middleware Home and Copying Oracle HTTP Server Files when Scaling Out

On the new node, mount the existing Middleware home.

Copy all files created in *ORACLE_INSTANCE*/config/OHS/*component*/moduleconf from the existing Web Tier configuration to the new one.

19.4.3 Running the Configuration Wizard to Configure the HTTP Server

Perform these steps to configure the Oracle Web Tier:

1. Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the file stage/Response/staticports.ini. Copy it to a file called ohs_ports.ini. Delete all entries in ohs_ports.ini except for OHS PORT and OPMN Local Port. Change the value of OPMN Local Port to 6700. If you are scaling out, you can use the default value, 7777, for OHS PORT. If you are scaling up, you must choose a unique value for that instance on the machine.

   Note: If the port names in the file are slightly different from OHS PORT and OPMN Local Port, use the names in the file.

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

   ```
   cd WEB_ORACLE_HOME/bin
   ```

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

   Ensure that Associate Selected Components with WebLogic Domain is selected.

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

   Click **Next**.
3. On the Specify WebLogic Domain Screen, enter
   - **Domain Host Name**: IADADMINVHN.mycompany.com

- **Domain Port No**: 7001, where 7001 is *IAD_WLS_PORT* in Section 11.1, "Assembling Information for Identity and Access Management Deployment."
- **User Name**: Weblogic Administrator User (For example: weblogic)
- **Password**: Password for the Weblogic Administrator User account

Click **Next**.

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

   Enter the following values for WEBHOST*n*, where *n* is the number of the new host, for example, 3:

   - **Instance Home Location**: *WEB_ORACLE_INSTANCE*, for example: /u02/local/oracle/config/instances/ohs1
   - **Instance Name**: web*n*
   - **OHS Component Name**: web*n*

   Click **Next**.

5. On the Configure Ports screen, you use the ohs_ports.ini file you created in Step 1to specify the ports to be used. This enables you to bypass automatic port configuration.

   a. Select **Specify Ports using a Configuration File**.

   b. In the file name field specify ohs_ports.ini.

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

6. On the Specify Security Updates screen, specify these values:

   - **Email Address**: The email address for your My Oracle Support account.
   - **Oracle Support Password**: The password for your My Oracle Support account.

   Select: **I wish to receive security updates via My Oracle Support**.

   Click **Next**.

7. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

   Click **Configure**.

   On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

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

19.4.4 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the new Oracle HTTP server, you must register the Oracle HTTP server with IAMAccessDomain. To do this, register Oracle HTTP Server with WebLogic Server by running the following command on the host where the new server is running:

```
cd WEB_ORACLE_INSTANCE/bin
./opmnctl registerinstance -adminHost IADADMINVHN.mycompany.com \
   -adminPort WLS_ADMIN_PORT -adminUsername weblogic
```

19.4.5 Reconfiguring the Load Balancer

Add the new Oracle HTTP Server instance to the existing server pool defined on the load balancer for distributing requests across the HTTP instances.

19.4.6 Scaling Up Oracle Traffic Director

To scale up Oracle traffic director:

1. Install Oracle Traffic Director on the new host as described in Section 12.2, "Installing Oracle Traffic Director on WEBHOST1 and WEBHOST2."
2. Create a new instance of Oracle Traffic Director on the new host as described in Section 12.4, "Register WEBHOST2 with the Administration Node."
3. Deploy the configuration to the new node by following the instructions in Section 12.11, "Deploying the Configuration and Testing the Virtual Server Addresses."
4. Create a new failover group for the new Oracle Traffic Director instance as described in Section 12.12, "Creating a Failover Group for Virtual Hosts."
5. Add the new Oracle Traffic Director failover group to the hardware load balancer pool.

19.5 Post-Scaling Steps for All Components

Perform the following post-scaling steps.

- Section 19.5.1, "Adding a New Managed Server to the Oracle Traffic Director Server Pool."
- Section 19.5.2, "Updating the Topology Store."
- Section 19.5.3, "Updating Stop/Start Scripts."
- Section 19.5.4, "Updating Node Manager Configuration."

19.5.1 Adding a New Managed Server to the Oracle Traffic Director Server Pool

The procedures described in this section show you how to add a new managed server or directory instance to an existing OTD server pool.

The following example is for OAM, but the process is the same for all managed servers/directory instances.

To add a third instance to the Oracle Traffic Director Access Manager server pool:

1. Log into the Oracle Traffic Director Administration Console.
2. Click **Server Pools** on the left panel.
3. Click the pool name, for example: **origin-server-pool-1**.
4. On the right panel, click **New Origin Server**.
5. Add the new Managed Server/Directory Instance, for example: **IAMHOST3, 14100** of the Origin Server.

   Click **Next**.
6. Click **New Origin Server**, and then **Close**.
7. Click **Deploy Changes** on the top of the panel.

19.5.2 Updating the Topology Store

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Lifecycle Tools read the store in order to build and execute the patch plan. If you scale out/up the topology you must add new entries to the store covering the new additions to the deployment.

To do this follow the steps in Appendix C, "Topology Tool Commands for Scaling."

19.5.3 Updating Stop/Start Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. When you create a new managed server in the domain you need to update the domain configuration so that these start and stop scripts can also start the newly created managed server.

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

19.5.4 Updating Node Manager Configuration

Update the node manager configuration, as described in the following sections:

- Section 19.5.4.1, "Starting and Stopping Node Manager."
- Section 19.5.4.2, "Setting Up Node Manager for an Enterprise Deployment."

19.5.4.1 Starting and Stopping Node Manager

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

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

For example:

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

If you want to start a managed server called WLS_OIM3 add an entry which looks like this:

```
newmachine.mycompany.com OIM ManagedServerName
```

For example:

```
OAMHOST3 OIM WLS_OIM3
```

Save the file.

If you added a new node manager, you must enable it for SSL as described in Section 19.5.4.2, "Setting Up Node Manager for an Enterprise Deployment."

19.5.4.2 Setting Up Node Manager for an Enterprise Deployment

This section describes how to configure Node Manager in accordance with Oracle best practice recommendations. It contains the following subsections:

- Section 19.5.4.2.1, "Enabling Host Name Verification Certificates for Node Manager."
- Section 19.5.4.2.2, "Generating Self-Signed Certificates Using the utils.CertGen Utility."

- Section 19.5.4.2.3, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."
- Section 19.5.4.2.4, "Creating a Trust Keystore Using the Keytool Utility."
- Section 19.5.4.2.5, "Configuring Node Manager to Use the Custom Keystores."
- Section 19.5.4.2.6, "Configuring Managed WebLogic Servers to Use the Custom Keystores."
- Section 19.5.4.2.7, "Changing the Host Name Verification Setting for the Managed Servers."
- Section 19.5.4.2.8, "Starting Node Manager."

19.5.4.2.1 Enabling Host Name Verification Certificates for Node Manager This section describes how to set up host name verification certificates for communication between Node Manager and the Administration Server.

19.5.4.2.2 Generating Self-Signed Certificates Using the utils.CertGen Utility The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST*.mycompany.com) and a WebLogic Managed Server listens on a virtual host name (*VIP*.mycompany.com). Whenever a server is using a virtual host name, it is implied that the server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example must be extended to:

1. Add the required host names to the certificate stores (if they are different from *HOST*.mycompany.com and *VIP*.mycompany.com).
2. Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by Managed Servers).

Follow these steps to create self-signed certificates on *HOST*. These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*. The following examples configure certificates for *HOST*.mycompany.com and *VIP*.mycompany.com; that is, it is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST*.mycompany.com is the address used by Node Manager and *VIP*.mycompany.com is the address used by a Managed Server or the Administration Server. This is the common situation for nodes hosting an Administration Server and a Fusion Middleware component, or for nodes where two Managed Servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the *WL_HOME*/server/bin/setWLSEnv.sh script. In the Bourne shell, run the following commands:

   ```
   cd WL_HOME/server/bin
   . ./setWLSEnv.sh
   ```

   Verify that the *CLASSPATH* environment variable is set:

   ```
   echo $CLASSPATH
   ```

2. Create a user-defined directory for the certificates. For example, create a directory called 'keystores' under the *ASERVER_HOME* directory. Note that certificates can be shared across WebLogic domains.

   ```
   cd SHARED_CONFIG
   mkdir keystores
   ```

   > **Note:** The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, for example).

3. Change directory to the directory that you just created:

   ```
   cd keystores
   ```

4. Using the `utils.CerGen` tool, create certificates for each Physical and Virtual Host in the topology.

   Syntax (all on a single line):

   ```
   java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
   [export | domestic] [Host_Name]
   ```

   Examples are:

   ```
   java utils.CertGen Key_Passphrase NEWHOST.mycompany.com_cert
   NEWHOST.mycompany.com_key domestic NEWHOST.mycompany.com
   ```

   Also create certificates for any new virtual hosts.

   ```
   java utils.CertGen Key_Passphrase NEWVHN.mycompany.com_cert
   NEWVHN.mycompany.com_key domestic NEWVHN.mycompany.com
   ```

19.5.4.2.3 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility Follow these steps when adding a new host:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, *ASERVER_HOME*/`keystores`).

   > **Note:** The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store using the `utils.ImportPrivateKey` utility.

2. Import the certificate and private key for each of the certificates created above into the Identity Store. Ensure that you use a different alias for each of the certificate/key pairs imported.

   Syntax (all on a single line):

   ```
   java utils.ImportPrivateKey Keystore_File Keystore_Password
   Certificate_Alias_to_Use Private_Key_Passphrase
   Certificate_File
   Private_Key_File
   ```

```
[Keystore_Type]
```

Examples:

```
java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityNEWHOST Key_Passphrase SHARED_
CONFIG/keystores/NEWHOST.mycompany.com_cert.pem SHARED_
CONFIG/keystores/NEWHOST.mycompany.com_key.pem
```

19.5.4.2.4 Creating a Trust Keystore Using the Keytool Utility Follow these steps to create a new Keystore for each new host.

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the *WL_HOME*/server/lib directory to the same directory as the certificates. For example:

```
cp WL_HOME/server/lib/cacerts SHARED_
CONFIG/keystores/appTrustKeyStoreNEWHOST.jks
```

2. The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password. Use the `keytool` utility to do this. The syntax is:

```
keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
Original_Password
```

For example:

```
keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStoreNEWHOST.jks
-storepass changeit
```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *WL_HOME*/`server/lib` directory. This CA certificate must be imported into the `appTrustKeyStore` using the `keytool` utility. The syntax is:

```
keytool -import -v -noprompt -trustcacerts -alias Alias_Name
-file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_
HOME/server/lib/CertGenCA.der -keystore appTrustKeyStoreNEWHOST.jks -storepass
Key_Passphrase
```

19.5.4.2.5 Configuring Node Manager to Use the Custom Keystores After adding a new node manager you need to configure it to use the new custom keystones described in Section 19.5.4.2.4, "Creating a Trust Keystore Using the Keytool Utility.". To configure Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` file located in the *SHARED_CONFIG*/nodemanager/*hostname* directory, where *hostname* is the name of the host where nodemanager runs:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=SHARED_CONFIG/keystores/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentityNEWHOST
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the `nodemanager.properties` file get encrypted when you start Node Manager as described in Section 20.1, "Starting and Stopping Components." For security reasons, minimize the time the entries in the `nodemanager.properties` file are left un-encrypted. After you edit the file, start Node Manager as soon as possible so that the entries get encrypted.

19.5.4.2.6 Configuring Managed WebLogic Servers to Use the Custom Keystores Follow these steps to configure the identity and trust keystores for *WLS_SERVER*:

1. Log in to Oracle WebLogic Server Administration Console for the for the domain which is being extended at: the address specified in Section 20.2, "About Identity and Access Management Console URLs."
2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Click the name of the server for which you want to configure the identity and trust keystores (*WLS_SERVER*). The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. In the Keystores field, select the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates.
8. In the Identity section, define attributes for the identity keystore:
   - **Custom Identity Keystore:** The fully qualified path to the identity keystore:

     ```
     SHARED_CONFIG/keystores/appIdentityKeyStore.jks
     ```

   - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
   - **Custom Identity Keystore Passphrase:** The password (*`Keystore_Password`*) you provided in Section 19.5.4.2.4, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.
9. In the Trust section, define properties for the trust keystore:
   - **Custom Trust Keystore:** The fully qualified path to the trust keystore:

     ```
     SHARED_CONFIG/keystores/appTrustKeyStoreNEWHOST.jks
     ```

   - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
   - **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in Section 19.5.4.2.4, "Creating a Trust Keystore Using the Keytool Utility" This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore.

However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.

10. Click **Save**.
11. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
12. Select **Configuration**, then **SSL**.
13. Click **Lock and Edit**.
14. In the **Private Key Alias** field, enter the alias you used for the host name the Managed Server listens on, for example: `appIdentityNEWHOST`

    In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 19.5.4.2.3, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."
15. Click **Save**.
16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
17. Restart the server for which the changes have been applied, as described in Section 20.1, "Starting and Stopping Components."

19.5.4.2.7 Changing the Host Name Verification Setting for the Managed Servers Once the previous steps have been performed, set host name verification for the affected Managed Servers to `Bea Hostname Verifier`. To do this, perform the following steps in both the IAMAccessDomain and IAMGovernanceDomain:

1. Log in to Oracle WebLogic Server Administration Console. (Console URLs are provided in Section 20.2, "About Identity and Access Management Console URLs.")
2. Select **Lock and Edit** from the change center.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select the Managed Server in the Names column of the table. The settings page for the server is displayed.
6. Open the SSL tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `Bea Hostname Verifier`.
9. Click **Save**.
10. Click **Activate Changes**.

19.5.4.2.8 Starting Node Manager Run the following commands to start Node Manager.

```
cd SHARED_CONFIG/nodemanager/hostname
./startNodeManagerWrapper.sh
```

Note: Verify that Node Manager is using the appropriate stores and alias from the Node Manager output. You should see the following when Node Manager starts.:

```
<Loading identity key store:
  FileName=ASERVER_HOME/keystores/appIdentityKeyStore.jks,
Type=jks, PassPhraseUsed=true>
```

Host name verification works if you apply a test configuration change to the servers and it succeeds without Node Manager reporting any SSL errors.

20

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the Identity and Access Management topology. These operations include monitoring, scaling, backing up your topology, and troubleshooting.

This chapter includes the following topics:

20.1 Starting and Stopping Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment.

This section contains the following topics:

20.1.1 Startup Order

When starting up your entire infrastructure, start the components in the following order, (ignoring those not in your topology):

1. Database(s)
2. Database Listener(s)
3. Web hosts
4. LDAP hosts
5. OAM hosts
6. OIM hosts
7. Oracle Identity Manager Managed servers
8. Identity Access Domain WebLogic Administration Server
9. Oracle Access Management Access Manager Server(s)
10. OAAM Administration Server
11. OAAM Managed Server (if OAAM is part of the topology)
12. Oracle HTTP Server(s)

20.1.2 Starting and Stopping All Servers by Using a Script

During Deployment, scripts were created in the `SHARED_CONFIG_DIR/config/scripts` directory to start and stop all the servers in the environment. Two of the scripts are available for you to use from the command line to start and stop all Identity and Access Management servers. The remaining scripts are used internally and must not be invoked from the command line.

Note:

- These scripts do NOT stop or start the database.
- These scripts do not stop or start Oracle Traffic Director. Start OTD manually, as described in Section 20.1.5, "Starting the Oracle Traffic Director Instances" before running these scripts.

20.1.2.1 Starting All Servers

Deployment created a file called `startall.sh`, which is used to start all of the components on a particular server. To start everything in the correct order run the command on hosts in the following order:

Exalogic Physical

- IAMHOST1
- IAMHOST2

Exalogic Logical

- OAMHOST1
- OIMHOST1
- OAMHOST2
- OIMHOST2

Exalogic Physical with OHS

- IAMHOST1

- IAMHOST2
- WEBHOST1
- WEBHOST2

If you want to start the services on a single host, execute the command on that host.

During exectution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

The script starts the components which are installed on a given host in the following order. What is started depends on what is installed on the host on which the script is running:

1. Oracle Unified Directory
2. Node Manager
3. Administration Server(s)
4. SOA Managed Server
5. OIM Managed Server
6. OAM Managed Server
7. Oracle HTTP Server
8. OAAM Managed Server

20.1.2.2 Stopping All Servers:

The script to stop all servers is `stopall.sh`.

Run the command on hosts in the reverse of the order used to start all servers.

During exectution you will be prompted to enter the Weblogic and Node Manager administrator passwords.

20.1.3 Manually Starting and Stopping Identity and Access Management Components

Oracle recommends using start and stop scripts to start and stop the components in a domain. If necessary however, it is possible to start components manually using the following procedures.

20.1.3.1 Starting and Stopping Oracle Unified Directory

Start and stop Oracle Unified Directory as follows:

20.1.3.1.1 Starting Oracle Unified Directory To start Oracle Unified Directory issue the following command:

```
OUD_ORACLE_INSTANCE/OUD/bin/start-ds
```

20.1.3.1.2 Stopping Oracle Unified Directory To stop Oracle Unified Directory issue the command:

```
OUD_ORACLE_INSTANCE/OUD/bin/stop-ds
```

20.1.3.2 Starting an Oracle Access Manager Managed Servers When None is Running

Normally, you start Access Manager managed servers by using the WebLogic console. After you have enabled Single Sign-On for the administration consoles, however, you must have at least one Access Manager Server running in order to access a console. If no Access Manager server is running, you can start one by using WLST.

To invoke WLST on Linux or UNIX, type:

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

Once you are in the WLST shell, execute the following commands:

```
nmConnect('Admin_User','Admin_Password', 'IADADMINVHN','Port', 'domain_name','IAD_
MSERVER_HOME')
nmStart('wls_oam1')
```

where *Port* is *NMGR_PORT*, *domain_name* is the name of the domain and *Admin_User* and *Admin_Password* are the Node Manager username and password. For example:

```
nmConnect('weblogic','password', 'IADADMINVHN','5556', 'IAMAccessDomain','IAD_
MSERVER_HOME')
```

If an Access Manager Managed server is already running then you can start the Access Manager Managed server as you would any other web logic managed server via the WebLogic Administration console.

20.1.3.3 Starting and Stopping a WebLogic Administration Server

Start and stop a WebLogic Administration Server as described in the following sections.

Notes:

- *Admin_User* and *Admin_Password* are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the file: *IAD_ASERVER_HOME*/config/nodemanager/nm_password.properties
- If you are starting the IAMAccessDomain Administration server, *ASERVER_HOME* is *IAD_ASERVER_HOME*. If you are starting the IAMGovernanceDomain Administration server, *ASERVER_HOME* is *IGD_ASERVER_HOME*

20.1.3.3.1 Starting a WebLogic Administration Server The recommended way to start the Administration server is to use WLST and connect to Node Manager:

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

Where *ORACLE_COMMON_HOME* is from the *MW_HOME* associated with the domain you are starting or stopping.

To start the Administration Server in the Access Domain, use the following command:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','IAD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('Admin_User','Admin_Password','IADADMINVHN','5556',
'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain')
nmStart('AdminServer')
```

Execute the following command to start the Administration Server in the Governance Domain:

```
nmConnect('Admin_User','Admin_Password','IGDADMINVHN','5556',
'IAMGovernanceDomain','IGD_ASERVER_HOME')
nmStart('AdminServer')
```

For example:

```
nmConnect('weblogic','password', 'IADADMINVHN','5556', 'IAMAccessDomain','IAD_
MSERVER_HOME')
```

Alternatively, you can start the Administration server by using the command:

```
ASERVER_HOME/bin/startWebLogic.sh
```

> **Note:** The Node Manager admin password is the *COMMON_IAM_PASSWORD*.

20.1.3.3.2 Stopping a WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console using the URL listed in Chapter 20.2, "About Identity and Access Management Console URLs."

Then proceed as follows:

1. Click the **Control** tab.
2. Select **AdminServer(admin)**.
3. Click **Shutdown** and select **Force Shutdown now**.
4. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

20.1.3.4 Starting and Stopping WebLogic Managed Servers

Start and stop managed servers as follows.

- Section 20.1.3.4.1, "Starting WebLogic Managed Servers"
- Section 20.1.3.4.2, "Stopping WebLogic Managed Servers"

> **Note:** The examples below use the WebLogic Console for starting and stopping managed servers. Once an environment has been provisioned and Single Sign-On enabled. Then in order to access the WebLogic Console at least one Oracle Access Manager managed server must be running. For starting and stopping Access Manager managed servers, see Section 20.1.3.2, "Starting an Oracle Access Manager Managed Servers When None is Running."

20.1.3.4.1 Starting WebLogic Managed Servers

To start a managed server, log in to the WebLogic console using the URL listed in Chapter 20.2, "About Identity and Access

Management Console URLs."

Then proceed as follows:

1. Click the **Control** tab.
2. Select **Environment -> Servers** from the Domain Structure menu.
3. Select managed server for example **wls_oim1**
4. Click the **Start** button.
5. Click **Yes** when asked to confirm that you want to start the server(s).

20.1.3.4.2 Stopping WebLogic Managed Servers To stop a Managed Server(s), log in to the WebLogic console using the URL listed in Chapter 20.2, "About Identity and Access Management Console URLs." Then proceed as follows:

1. Select **Environment -> Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select Managed Server for example **wls_oim1**
4. Click the **Shutdown** button and select **Force Shutdown Now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

20.1.3.5 Starting and Stopping Node Manager

Start and stop Node Manager as follows.

20.1.3.5.1 Starting Node Manager If the Node Manager being started is the one that controls the Administration Server, then prior to starting the Node Manager issue the command:

```
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
```

To start Node Manager, issue the commands:

```
cd SHARED_CONFIG_DIR/nodemanager/hostname
./startNodeManagerWrapper.sh
```

20.1.3.5.2 Stopping Node Manager To stop Node Manager, kill the process started in the previous section.

20.1.4 Stopping and Starting vServers

Stop and start vServers as follows.

20.1.4.1 Stopping vServers

To stop a vServer, do the following:

Note: Do not use the `xm destroy` command or Oracle VM Manager to stop a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Under vDCs, expand your cloud such as `MyCloud`.

4. Expand **Accounts**.
5. Expand the name of your account, such as `Dept1`.
   All the vServers in the account are displayed.
6. Select the **vServer** you wish to stop.
   The dashboard of the vServer is displayed.
7. From the actions pane on the right, click **Stop vServer**. Wait till the job succeeds in the jobs pane.

20.1.4.2 Starting vServers

To start a vServer, do the following:

> **Note:** Do not use the `xm create` command or Oracle VM Manager to start a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Expand your cloud, such as `MyCloud`.
4. Expand **Accounts**.
5. Expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.
6. Select the **vServer** you wish to start.

   The dashboard of the vServer is displayed.
7. From the actions pane on the right, click **Start vServer**. Wait till the job succeeds in the jobs pane.

20.1.5 Starting the Oracle Traffic Director Instances

To start Oracle Traffic Director instances using the administration console:

1. Log in to the administration console using the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. Click the **Configurations** button that is situated at the upper left corner of the page.

   A list of the available configurations is displayed.
3. Select the configuration for which you want to start the instance.
4. In the navigation pane, select **Instances**.
5. Click the **Start/Restart** button for the instance that you want to start.

20.1.5.1 Starting and Stopping Oracle Traffic Director Administration Instances

OTD administration instances must be running to enable access to the OTD administration console and to enable the administration console to control remote OTD instances. To start the OTD administration console: perform the following steps.

Execute the command `startserv` located in the directory: *`WEB_ORACLE_INSTANCE`*`/admin-server/bin`

To stop the Administration Services, execute the command `stopserv` located in the directory: *`WEB_ORACLE_INSTANCE`*`/admin-server/bin`

> **Note:** If you are not running Oracle Traffic Director as root, manually stop the OTD failover groups first using the following command:
>
> ```
> OTD_ORACLE_HOME/bin/tadm stop-failover --instance-home=WEB_
> INSTANCE_HOME/ --config=sso.mycompany.com
> ```

20.1.5.2 Starting Oracle Traffic Director Instances

To start or restart *all* instances of the selected configuration, click **Start/Restart Instances** in the Common Tasks pane. To stop all instances of the configuration, click **Stop Instances**.

20.1.5.3 Starting Oracle Traffic Director Failover groups

If you started your OTD instances as the software owner rather than `root`, then start OTD failover groups using the following command when you are logged in as `root`:

```
WEB_ORACLE_HOME/bin/tadm start-failover --instance-home=WEB_INSTANCE_HOME/
--config=IAM
```

If you did not configure your Oracle Traffic Director to start as root, manually start the failover groups using the following command as root:

```
OTD_ORACLE_HOME/bin/tadm start-failover --instance-home=WEB_INSTANCE_HOME/
--config=sso.mycompany.com
```

20.2 About Identity and Access Management Console URLs

Table 20–1 lists the administration consoles used in this guide and their URLs.

Table 20–1 Console URLs

Domain	Console	URL	User Name
IAMAccessDomain	WebLogic Administration Console	`http://IADADMIN.mycompany.com/console`	`weblogic_idm`
	Enterprise Manager FMW Control	`http://IADADMIN.mycompany.com/em`	`weblogic_idm`
	Access Management console	`http://IADADMIN.mycompany.com/oamconsole`	`oamadmin`
	OAAM Server	`https://SSO.mycompany.com/oaam_server`	`oaamadmin`
	OAAM Administration Console	`http://IADADMIN.mycompany.com/oaam_admin`	`oaamadmin`
IAMGovernanceDomain	WebLogic Administration Console	`http://IGDADMIN.mycompany.com/console`	`weblogic_idm`

Table 20–1 (Cont.) Console URLs

Domain	Console	URL	User Name
	Enterprise Manager FMW Control	`http://IGDADMIN.mycompany.com/em`	`weblogic_idm`
	Identity Manager System Administration Console	`http://IGDADMIN.mycompany.com/sysadmin`	`xelsysadm`
	Oracle Identity Self Service	`https://SSO.mycompany.com/identity`	`xelsysadm`
	Authorization Policy Manager	`http://IGDADMIN.mycompany.com/apm`	`oamadmin`
N/A	Exalogic Control (Enterprise Manager Operations Control)	`https://exalogic:9943/emoc`	
N/A	Oracle Traffic Director Administration Console	`https://OTDADMINVHN.mycompany.com:8989`	`otdadmin`
N/A	Oracle ZFS Storage Appliance Browser User Interface	https://*exalogicsn01-priv*:215	

20.3 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 20.3.1, "Monitoring Oracle Unified Directory"
- Section 20.3.2, "Monitoring WebLogic Managed Servers"

20.3.1 Monitoring Oracle Unified Directory

You can check the status of Oracle Unified Directory by issuing the command:

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

This command prompts for the OUD Admin username and *OUD_COMMON_PASSOWORD*.

This command accesses the locally running Oracle Unified Directory instance and reports the status of the directory, including whether or not replication and LDAP or LDAPS is enabled.

20.3.2 Monitoring WebLogic Managed Servers

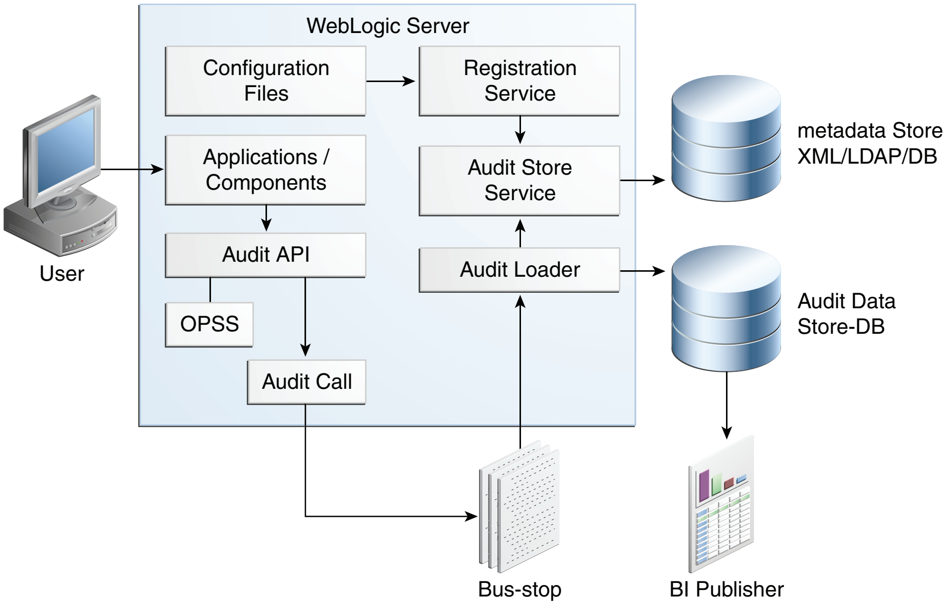
You can use Oracle Enterprise Manager Fusion Middleware Control to monitor Managed Servers and other Fusion Middleware components, such as Access Manager, Oracle Identity Manager, Oracle Identity Federation, and SOA. For more information, see the administrator guides listed in the Preface under "Related Documents".

20.4 Auditing Identity and Access Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications are able to create application-specific audit events. For non-JavaEE Oracle components in the middleware such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

Figure 20–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework. For more information, see *Oracle Fusion Middleware Security Guide*.

Figure 20–1 Audit Event Flow



The Oracle Fusion Middleware Audit Framework consists of the following key components:

- Audit APIs

  These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run-time, applications may call these APIs where appropriate to audit the necessary information about a particular event happening in the application code. The interface enables applications to specify event details such as username and other attributes needed to provide the context of the event being audited.

- Audit Events and Configuration

The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also enables applications to define application-specific events.

These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WLST (command-line tool).

- The Audit Bus-stop

  Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are periodically uploaded to the audit repository based on a configurable time interval.

- Audit Loader

  As the name implies, audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.

- Audit Repository

  Audit Repository contains a pre-defined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and grow over time. Ideally, this should not be an operational database used by any other applications - rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (Oracle RAC) database as the audit data store.

- Oracle Business Intelligence Publisher

  The data in the audit repository is exposed through pre-defined reports in Oracle Business Intelligence Publisher. The reports enable users to drill down the audit data based on various criteria. For example:

  - Username
  - Time Range
  - Application Type
  - Execution Context Identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware 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 are available once the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

20.5 Performing Backups and Recoveries

You can use the UNIX `tar` command for most backups. Typical usage is:

```
tar -czvpsPf BACKUP_LOCATION/backup_file.tar directories
```

You can use the UNIX `tar` command for recovery. Typical usage is:

```
tar -xzvpsPf BACKUP_LOCATION/backup_file.tar
```

For database backup and recovery, you can use the database utility RMAN. See the *Oracle Database Backup and Recovery Reference* for more information on using this command.

This section contains the following topics:

- Section 20.5.1, "Peforming Baseline Backups"
- Section 20.5.2, "Performing Runtime Backups"
- Section 20.5.3, "Performing Backups During Installation and Configuration"

20.5.1 Peforming Baseline Backups

Perform baseline backups when building a system and when applying patches that update static artifacts, such as the Oracle binaries.

After performing a baseline backup, also perform a runtime backup.

Table 20–2 Static Artifacts to Back Up in the Identity and Access Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	Oracle RAC database hosts: IAMDBHOST1 IAMDBHOST2	User Defined	Database
Oracle Unified Directory Binaries	LDAPHOST1 LDAPHOST2	Middleware Home: `DIR_MW_HOME`	Directory Tier
Oracle Access Management Binaries	OAMHOST1 OAMHOST2	Middleware Home: *`IAD_MW_HOME`*	Application Tier
Oracle Identity Governance Binaries	OIMHOST1 OIMHOST2	Middleware Home: *`IGD_MW_HOME`*	Application Tier
Web Tier Binaries	WEBHOST1 WEBHOST2	Middleware Oracle home, *`WEB_ORACLE_HOME`*:	Web Tier

Install-Related Files	Each host	OraInventory:
		`ORACLE_BASE``/oraInventory`
		`/etc/oratab`, `/etc/oraInst.loc`
		`~/bea/beahomelist` (on hosts where WebLogic Server is installed)
			Not applicable.

Note: It is also recommended that you back up your load balancer configuration. Refer to your vendor documentation on how to do this.

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

20.5.2 Performing Runtime Backups

Perform runtime backups on an ongoing basis. These backups contain information on items that can change frequently, such as data in the database, domain configuration information, and identity information in LDAP directories.

Table 20–3 Run-Time Artifacts to Back Up in the Identity and Access Management Enterprise Deployments

Type	Host	Location	Tier
IAMAccessDomain Home	OAMHOST1 OAMHOST2	Administration Server and Shared Files: *IAD_ASERVER_HOME* Managed Servers: *IAD_MSERVER_HOME*	Application Tier
IAMGovernanceDomain Home	OIMHOST1 OIMHOST2	Administration Server and Shared Files: *IGD_ASERVER_HOME* Managed Servers: *IGD_MSERVER_HOME*	Application Tier
Oracle HTTP Server	WEBHOST1 WEBHOST2	*WEB_ORACLE_INSTANCE*	Web Tier
Oracle RAC Databases	IAMDBHOST1 IAMDBHOST2	User defined	Directory Tier
Oracle Unified Directory	LDAPHOST1 LDAPHOST2	*OUD_ORACLE_INSTANCE*	Application Tier

20.5.3 Performing Backups During Installation and Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process.

For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

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

This section contains the following topics:

- Section 20.5.3.1, "Backing Up Middleware Home"
- Section 20.5.3.2, "Backing Up LDAP Directories"
- Section 20.5.3.3, "Backing Up the Database"
- Section 20.5.3.4, "Backing Up the WebLogic Domain IAMGovernanceDomain"

- Section 20.5.3.5, "Backing Up the WebLogic Domain IAMAccessDomain"
- Section 20.5.3.6, "Backing Up the Web Tier"

20.5.3.1 Backing Up Middleware Home

Back up the Middleware homes whenever you create a new one or add components to it. The Middleware homes used in this guide are Oracle Identity Management and Oracle Identity and Access Management, as listed in Table 20–2.

20.5.3.2 Backing Up LDAP Directories

Whenever you perform an action which updates the data in LDAP, back up the directory contents.

This section contains the following topics:

- Section 20.5.3.2.1, "Backing Up Oracle Unified Directory"
- Section 20.5.3.2.2, "Backing Up Third-Party Directories"

20.5.3.2.1 Backing Up Oracle Unified Directory To backup Oracle Unified Directory, perform the following steps:

1. Shut down the Oracle Unified Directory Instances as described in Section 20.1, "Starting and Stopping Components."
2. Back up *OUD_ORACLE_INSTANCE* directories on each host.
3. Restart the Oracle Unified Directory instances as described in Section 20.1, "Starting and Stopping Components."

20.5.3.2.2 Backing Up Third-Party Directories Refer to your operating system vendor's documentation for information about backing up directories.

20.5.3.3 Backing Up the Database

Whenever you create add a component to the configuration, back up the IAMDB database. Perform this backup after creating domains or adding components such as Oracle Access Management Access Manager or Oracle Identity Manager.

20.5.3.4 Backing Up the WebLogic Domain IAMGovernanceDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 20.1, "Starting and Stopping Components."
2. Back up the *IGD_ASERVER_HOME* directory from shared storage.
3. Back up the *IGD_MSERVER_HOME* directory from each host.
4. Restart the WebLogic Administration Server and managed servers.

20.5.3.5 Backing Up the WebLogic Domain IAMAccessDomain

To back up the WebLogic domain, perform these steps:

1. Shut down the WebLogic administration server and any managed servers running in the domain as described in Section 20.1, "Starting and Stopping Components."
2. Back up the *IAD_ASERVER_HOME* directory from shared storage.
3. Back up the *IAD_MSERVER_HOME* directory from each host.

4. Restart the WebLogic Administration Server and managed servers.

20.5.3.6 Backing Up the Web Tier

To back up the Web Tier, perform these steps:

20.5.3.6.1 Backing Up Oracle HTTP Server

Back up Oracle HTTP Server as follows:

1. Shut down the Oracle HTTP Server as described in Section 20.1, "Starting and Stopping Components."
2. Back up the *WEB_ORACLE_INSTANCE* directory on local storage.
3. Start the Oracle HTTP Server as described in Section 20.1, "Starting and Stopping Components."

20.5.3.6.2 Backing Up Oracle Traffic Director

To back up the Oracle Traffic Director Administration Server, run the following command on WEBHOST1:

```
tar -cvpf webasback.tar WEB_ORACLE_INSTANCE
```

20.6 Patching Enterprise Deployments

It is recommended that you patch enterprise deployments by using the automated patching solution included with the Identity and Access Management Lifecycle Tools.

The process of applying patches can be summarized as follows:

1. Create a patch top. A patch top directory contains patches, classified by each product to which patches apply.
2. Run Patch Manager to generate a patch plan. Based on the deployment topology and patches provided, the Manager creates an optimal plan to apply those patches.
3. Run the Patcher against all hosts which are affected by the plan. You might need to execute the Patcher on a given host multiple times if required by a given plan. As each Patcher invocation completes, it directs you where to run the Patcher next.

When the Patcher runs, it stops and starts server instances as necessary, and ensures that patches are applied in the correct order to satisfy dependencies.

Full details on how to use the IDM Patching Framework can be found in *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*. The Guide also contains instructions for patching the deployment manually if required, using the OPatch tool.

20.7 Preventing Timeouts for SQL

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall so it does not time out these connections. If such a configuration is not possible, set the SQLNET.EXPIRE_TIME=n parameter in the `ORACLE_HOME/network/admin/sqlnet.ora` file on the database server, where `n` is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

20.8 Manually Failing Over the WebLogic Administration Server

This section discusses how to fail over the Administration Server to a new host after the primary host fails. The example in this section shows how to fail the Access Management Administration Server from OAMHOST1 to OAMHOST2. If you are failing over the Oracle Identity Manager Administration server, substitute the appropriate values for that domain.

This section contains the following topics:

- Section 20.8.1, "Failing Over the Administration Server to OAMHOST2"
- Section 20.8.2, "Starting the Administration Server on OAMHOST2"
- Section 20.8.3, "Validating Access to OAMHOST2 Through Oracle HTTP Server"
- Section 20.8.4, "Failing the Administration Server Back to OAMHOST1"

20.8.1 Failing Over the Administration Server to OAMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from OAMHOST1 to OAMHOST2.

Assumptions:

- The Administration Server is configured to listen on `IADADMINVHN.mycompany.com`, and not on `ANY` address.
- The Administration Server is failed over from OAMHOST1 to OAMHOST2, and the two nodes have these IP addresses:
  - OAMHOST1: `100.200.140.165`
  - OAMHOST2: `100.200.140.205`
  - IADADMINVHN: `100.200.140.206`

    This is the Virtual IP address where the Administration Server is running, assigned to *interface*:*index* (for example, eth1:2), available in OAMHOST1 and OAMHOST2.
- The domain directory where the Administration Server is running in OAMHOST1 is on a shared storage and is mounted also from OAMHOST2.

  > **Note:** NM in OAMHOST2 does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on OAMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, Node Manager is fully functional

- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed in OAMHOST2 as described in previous chapters. That is, the same path for *`IAD_ORACLE_HOME`* and *`IAD_MW_HOME`* that exists in OAMHOST1 is available in OAMHOST2.

The following procedure shows how to fail over the Administration Server to a different node, OAMHOST2.

1. Stop the Administration Server on OAMHOST1 as described in Section 20.1, "Starting and Stopping Components."
2. Migrate the IP address to the second node.

a. Run the following command as root on OAMHOST1 (where *x*:*y* is the current interface used by `IADADMINVHN.mycompany.com`):

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

For example:

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

b. Run the following command on OAMHOST2:

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

For example:

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

> **Note:** Ensure that the netmask and interface to be used match the available network configuration in OAMHOST2.

3. Update routing tables by using `arping` on OAMHOST2, for example:

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

20.8.2 Starting the Administration Server on OAMHOST2

Perform the following steps to start Node Manager on OAMHOST2.

1. On OAMHOST2, mount the Administration Server domain directory if it is not already mounted. For example:

```
mount /u01/oracle
```

2. Start Node Manager by using the following commands:

```
cd WL_HOME/server/bin
./startNodeManager.sh
```

3. Stop the Node Manager by killing the Node Manager process.

> **Note:** Starting and stopping Node Manager at this point is only necessary the first time you run Node Manager. Starting and stopping it creates a property file from a predefined template. The next step adds properties to that property file.

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

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

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

5. Start the Node Manager as described in Section 20.1, "Starting and Stopping Components."

6. Start the Administration Server on OAMHOST2.

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

   Once in the WLST shell, execute the following commands:

   ```
   nmConnect('admin','Admin_Password', 'OAMHOST2','5556',
   'IAMAccessDomain','/u1/oracle/config/domains/IAMAccessDomain')
   nmStart('AdminServer')
   ```

7. Test that you can access the Administration Server on OAMHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console at:

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

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

20.8.3 Validating Access to OAMHOST2 Through Oracle HTTP Server

Perform the same steps as in Section 16.1.1, "Verify Connectivity" This is to check that you can access the Administration Server when it is running on OAMHOST2.

20.8.4 Failing the Administration Server Back to OAMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on OAMHOST2 and run it on OAMHOST1. To do this, migrate IADADMINVHN back to OAMHOST1 node as described in the following steps.

1. Ensure that the Administration Server is not running on OAMHOST2. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from *`IAD_ASERVER_HOME`*`/bin`.

2. On OAMHOST2, unmount the Administration server domain directory. For example:

   ```
   umount /u01/oracle
   ```

3. On OAMHOST1, mount the Administration server domain directory. For example:

   ```
   mount /u01/oracle
   ```

4. Disable the `IADADMINVHN.mycompany.com` virtual IP address on OAMHOST2 and run the following command as `root` on OAMHOST2:

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

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

5. Run the following command on OAMHOST1:

   ```
   /sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
   ```

   Note: Ensure that the netmask and interface to be used match the available network configuration in OAMHOST1

6. Update routing tables by using arping. Run the following command from OAMHOST1.

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

7. If Node Manager is not already started on OAMHOST1, start it, as described in Section 20.1, "Starting and Stopping Components."

8. Start the Administration Server again on OAMHOST1.

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

   Once in the WLST shell, execute

   ```
   nmConnect(admin,'Admin_Pasword, OAMHOST1,'5556',
        'IAMAccessDomain','/u01/oracle/config/domains/IAMAccessDomain'
   nmStart('AdminServer')
   ```

9. Test that you can access the Oracle WebLogic Server Administration Console at:

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

   where `7001` is *`WLS_ADMIN_PORT`* in Section 11.1, "Assembling Information for Identity and Access Management Deployment."

10. Check that you can access and verify the status of components in the Oracle Enterprise Manager at:

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

20.9 Changing Startup Location

When the environment was deployed, start and stop scripts were generated to start and stop components in the topology. At the time of Deployment, the Access Domain Administration server was configured to start on OAMHOST1. If you want to permanently change this to start on OAMHOST2, perform the following steps.

Use the same steps, changing the name of the server and host, to change the Governance Domain Administration server to start on OIMHOST2 instead of OIMHOST1.

Edit the file `serverInstancesInfo.txt`, which is located in the directory: *`SHARED_CONFIG_DIR`*`/scripts`

Locate the line which looks like this:

```
OAMHOST1.mycompany.com AS AdminServer
```

Change `OAMHOST1` to `OAMHOST2` and save the file.

20.10 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity and Access Management enterprise deployment described in this manual.

This section contains the following topics:

- Section 20.10.1, "Troubleshooting Oracle Traffic Director"
- Section 20.10.2, "Troubleshooting Identity and Access Management Deployment"
- Section 20.10.3, "Troubleshooting Start/Stop Scripts"

- Section 20.10.4, "Troubleshooting Oracle Oracle Access Management Access Manager 11g"
- Section 20.10.5, "Troubleshooting Oracle Identity Manager"
- Section 20.10.6, "Troubleshooting Oracle SOA Suite"

20.10.1 Troubleshooting Oracle Traffic Director

This section describes possible issues for Oracle Traffic Director (OTD).

Problem

OTD failover groups show as started, but IP address cannot be pinged.

Failover groups require a distinct Router ID on the system. If you reuse a Router ID, this behavior occurs. This can even occur if you remove and reinstall OTD.

Solution

To resolve this issue, recreate the failover group using a different Router ID

20.10.2 Troubleshooting Identity and Access Management Deployment

This section describes some common problems related to Deployment. It contains the following topics:

- Section 20.10.2.1, "Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute"
- Section 20.10.2.2, "Deployment Fails"
- Section 20.10.2.3, "Connection to Directory Failed Exception"

20.10.2.1 Deployment Fails with Error: Incorrect Host or Domain Name Format for Attribute

Problem

Deployment fails with an error similar to this:

```
Incorrect host format for attibute : PRIMARY_OAM_SERVERS :
server-123.mycompany.com
```

Due to a bug, one of the tools invoked during the deployment process cannot handle host names or domain names containing the hyphen (**-**) character.

Solution

Use host names and domain names that do NOT contain the hyphen (**-**) character.

20.10.2.2 Deployment Fails

Problem

Deployment fails.

Solution

Check the Deployment logs located in the directory:

`LCM_HOME``/provisioning/logs/`*`hostname`*

where *`hostname`* is the host where the Deployment step failed.

Rectify the error, clean up the environment and re-deploy.

For information about cleaning up the environment, see Appendix B, "Cleaning Up an Environment Before Rerunning IAM Deployment."

20.10.2.3 Connection to Directory Failed Exception

Problem

You see the following error in the log configure log file:

```
oracle.idm.automation.exception.ExecutionFailedException: Connection to Directory
failed: Host/Port details incorrect
```

Solution

1. Check the property file mentioned in the log file output.

   A line similar to the following appears a bit farther in the log:

   ```
   See [/u01/oracle/products/products/access/iam/idmtools/bin/idmConfigTool.sh,
   -configOAM, input_
   file=/u01/lcm/tools/idmlcm/provisioning/idm-provisioning-build/config/config_
   oam.properties, log_
   file=/u01/lcm/provisioning/logs/slcn04cn10.mycompany.com/idmautomation-configOA
   M.log, log_level=FINEST]{3}
   ```

   From this output you can see that the property file is called `config_oam.properties`. This file however, is moved from the location stated to the log directory. Examine this file and check that the entries `IDSTORE_HOST`/`IDSTORE_PORT` reference your load balancer/OTD directory entry (`LBR_LDAP_HOST`/`LBR_LDAP_PORT`).

2. Validate that you can connect to the directory on the local host by telnetting to the LDAP_HOST and LDAP_PORT for example.

   ```
   telnet ldaphost1 1389
   ```

   If you see an entry similar to:

   ```
    Trying 10.245.169.148...
         Connected to slcn04cn10.mycompany.com (10.245.169.148).
         Escape character is '^]'.
   ```

   Then you know that the directory was configured and is running.

   If it is not, the directory was not successfully configured, Check the standard directory log files for more information.

3. Check that you can connect to the directory using the load balancer or OTD entry using `LBR_LDAP_HOST` and `LBR_LDAP_PORT` for example:

   ```
   telnet idstore.mycompany.com 389
   ```

   If you don't see a connection, your load balancer or OTD instance is incorrectly configured. Recheck the configuration.

20.10.3 Troubleshooting Start/Stop Scripts

This section describes some common problems related to Start/Stop scripts. It contains the following topics:

- Section 20.10.3.1, "Preverify Inappropriately Fails with Insufficient Space"

- Section 20.10.3.2, "Start/Stop Scripts Fail to Start or Stop a Managed Server"

20.10.3.1 Preverify Inappropriately Fails with Insufficient Space

Problem

When preverify runs, it checks that sufficient space is available in the directory *IDM_TOP*. If you have created separate mount points for *IDM_TOP*/products and *IDM_TOP*/config, preverify does not add together the space allocated to the two mount points and fails the check inappropriately.

Solution

Disable the free space check by editing the file:

```
LCM_
HOME/provisioning/idm-provisioning-build/idm-common-preverify-build.xml
```

Locate the entry:

```
<target name="common-preverify-tasks">
```

Comment out the following entry so that after editing it looks like this:

```
        <!--antcall target="private-preverify-free-space"/-->
```

Save the file.

20.10.3.2 Start/Stop Scripts Fail to Start or Stop a Managed Server

Problem

Problem: Start/Stop scripts fail to start or stop a managed server.

The start/stop logs in the directory *SHARED_CONFIG_DIR*/scripts/logs contain an error similar to this:

```
weblogic.utils.AssertionError: ***** ASSERTION FAILED *****
        at
weblogic.server.ServerLifeCycleRuntime.getStateRemote(ServerLifeCycleRuntime.java:
734)
        at
weblogic.server.ServerLifeCycleRuntime.getState(ServerLifeCycleRuntime.java:581)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

Solution

1. Shut down the failing managed server. You might have to kill the process.
2. Back up the managed server's LDAP data, then remove it. For example:

   ```
   rm -rf LOCAL_CONFIG_DIR/domains/IAMAccessDomain/servers/server_name/data/ldap
   ```

   where *server_name* is the name of the failing managed server.
3. Restart the managed server.

20.10.4 Troubleshooting Oracle Oracle Access Management Access Manager 11g

This section describes some common problems that can arise with Access Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 20.10.4.1, "Access Manager Runs out of Memory"
- Section 20.10.4.2, "User Reaches the Maximum Allowed Number of Sessions"
- Section 20.10.4.3, "Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed"
- Section 20.10.4.4, "You Are Not Prompted for Credentials After Accessing a Protected Resource"
- Section 20.10.4.5, "Cannot Log In to Access Management Console"

20.10.4.1 Access Manager Runs out of Memory

Problem

After Access Manager has been running for a while, you see the following error message in the output:

```
Attempting to allocate 1G bytes
There is insufficient native memory for the Java Runtime Environment to continue.
```

Possible reasons:

- The system is out of physical RAM or swap space.
- In 32 bit mode, the process size limit was reached.

Solutions

- Reduce memory load on the system.
- Increase physical memory or swap space.
- Check if swap backing store is full.
- Use 64 bit Java on a 64 bit OS.
- Decrease Java heap size (-Xmx/-Xms).
- Decrease number of Java threads.
- Decrease Java thread stack sizes (-Xss).
- Disable compressed references (-XXcompressedRefs=false).
- Ensure that command line tool `adrci` can be executed from the command line.
  - at oracle.dfw.impl.incident.ADRHelper.invoke(ADRHelper.java:1309)
  - at oracle.dfw.impl.incident.ADRHelper.createIncident(ADRHelper.java:929
  - at oracle.dfw.impl.incident.DiagnosticsDataExtractorImpl.createADRIncident(DiagnosticsDataExtractorImpl.java:1116)
- On both OAMHOST1 and OAMHOST2, edit the file `setSOADomainEnv.sh`, which is located in *`IAD_MSERVER_HOME`*`/bin` and locate the line which begins:

  ```
  PORT_MEM_ARGS=
  ```

  Change this line so that it reads:

  ```
  PORT_MEM_ARGS="-Xms768m -Xmx2560m"
  ```

20.10.4.2 User Reaches the Maximum Allowed Number of Sessions

Problem

The Access Manager server displays an error message similar to this:

```
The user has already reached the maximum allowed number of sessions. Please close
one of the existing sessions before trying to login again.
```

Solution

If users log in multiple times without logging out, they might overshoot the maximum number of configured sessions. You can modify the maximum number of configured sessions by using the Access Management Administration Console.

To modify the configuration by using the Access Management Administration Console, proceed as follows:

1. Go to **System Configuration** -> **Common Settings** -> **Session**
2. Increase the value in the **Maximum Number of Sessions per User** field to cover all concurrent login sessions expected for any user. The range of values for this field is from 1 to any number.

20.10.4.3 Policies Do Not Get Created When Oracle Access Management Access Manager is First Installed

Problem

The Administration Server takes a long time to start after configuring Access Manager.

Solution

Tune the Access Manager database. When the Administration server first starts after configuring Access Manager, it creates a number of default policies in the database. If the database is distant or in need of tuning, this can take a significant amount of time.

```
Resources
Authentication Policies
   Protected Higher Level Policy
   Protected Lower Level Policy
   Publicl Policy
Authorization Policies
   Authorization Policies
```

If you do not see these items, the initial population has failed. Check the Administration Server log file for details.

20.10.4.4 You Are Not Prompted for Credentials After Accessing a Protected Resource

Problem

When you access a protected resource, Access Manager should prompt you for your user name and password. For example, after creating a simple HTML page and adding it as a resource, you should see credential entry screen.

Solution

If you do not see the credential entry screen, perform the following steps:

1. Verify that Host Aliases for IAMAccessDomain have been set. You should have aliases for `IAMAccessDomain`:80, `IAMAccessDomain`:Null, `IADADMIN.mycompany.com:80`, and `SSO.mycompany.com:443`, where Port `80` is *`HTTP_PORT`* and Port `443` is *`HTTP_SSL_PORT`*.
2. Verify that WebGate is installed.
3. Verify that `ObAccessClient.xml` was copied from *`IAD_ASERVER_HOME`*`/output` to the WebGate Lib directory and that OHS was restarted.
4. When `ObAccessClient.xml` was first created, the file was not formatted. When the OHS is restarted, reexamine the file to ensure that it is now formatted. OHS gets a new version of the file from Access Manager when it first starts.
5. Shut down the Access Manager servers and try to access the protected resource. You should see an error saying Access Manager servers are not available. If you do not see this error, re-install WebGate.

20.10.4.5 Cannot Log In to Access Management Console

Problem

You cannot log in to the Access Management Console. The Administration Server diagnostic log might contain an error message similar to this:

```
Caused by: oracle.security.idm.OperationFailureException:
oracle.security.am.common.jndi.ldap.PoolingException [Root exception is
oracle.ucp.UniversalConnectionPoolException:
Invalid life cycle state.
 Check the status of the Universal Connection Pool]
        at
oracle.security.idm.providers.stdldap.UCPool.acquireConnection(UCPool.java:112)
```

Solution

Remove the /tmp/UCP* files and restart the Administration Server.

20.10.5 Troubleshooting Oracle Identity Manager

This section describes some common problems that can arise with Oracle Identity Manager and the actions you can take to resolve the problem. It contains the following topics:

- Section 20.10.5.1, "java.io.FileNotFoundException When Running Oracle Identity Manager Configuration"
- Section 20.10.5.2, "ResourceConnectionValidationxception When Creating User in Oracle Identity Manager"
- Section 20.10.5.3, "Oracle Identity Manager Reconciliation Jobs Fail"

20.10.5.1 java.io.FileNotFoundException When Running Oracle Identity Manager Configuration

Problem

When you run Oracle Identity Manager configuration, the error `java.io.FileNotFoundException: soaconfigplan.xml (Permission denied`) may appear and Oracle Identity Manager configuration might fail.

Solution

To workaround this issue:

1. Delete the file `/tmp/soaconfigplan.xml`.
2. Start the configuration again (`OH/bin/config.sh`).

20.10.5.2 ResourceConnectionValidationxception When Creating User in Oracle Identity Manager

Problem

If you are creating a user in Oracle Identity Manager (by logging into Oracle Identity Manager System Administration Console, clicking the Administration tab, clicking the **Create User** link, entering the required information in the fields, and clicking **Save**) in an active-active Oracle Identity Manager configuration, and the Oracle Identity Manager server that is handling the request fails, you may see a "ResourceConnectionValidationxception" in the Oracle Identity Manager log file, similar to:

```
[2010-06-14T15:14:48.738-07:00] [oim_server2] [ERROR] [] [XELLERATE.SERVER]
[tid: [ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: xelsysadm] [ecid:
004YGJGmYrtEkJV6u3M6UH00073A0005EI,0:1] [APP: oim#11.1.1.3.0] [dcid:
12eb0f9c6e8796f4:-785b18b3:12938857792:-7ffd-0000000000000037] [URI:
/admin/faces/pages/Admin.jspx] Class/Method:
PooledResourceConnection/heartbeat encounter some problems: Operation timed
out[[
com.oracle.oim.gcp.exceptions.ResourceConnectionValidationxception: Operation
timed out
        at
oracle.iam.ldapsync.impl.repository.LDAPConnection.heartbeat(LDAPConnection.ja
va:162)
        at
com.oracle.oim.gcp.ucp.PooledResourceConnection.heartbeat(PooledResourceConnec
tion.java:52)
         .
         .
         .
```

Solution

Despite this exception, the user is created correctly.

20.10.5.3 Oracle Identity Manager Reconciliation Jobs Fail

Problem

Oracle Identity Manager reconciliation jobs fail, or the following message is seen in the log files:

```
LDAP Error 53 : [LDAP: error code 53 - Full resync required. Reason: The provided
cookie is older than the start of historical in the server for the replicated
domain : dc=mycompany,dc=com]
```

This error is caused by the data in the Oracle Unified Directory change log cookie expiring because Oracle Unified Directory has not been written to for a certain amount of time.

Solution:

1. Open a browser and go to the following location:

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

2. Log in a as `xelsysadm` using the *`COMMON_IDM_PASSWORD`*.
3. Under **System Management**, click **Scheduler**.
4. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.
5. For each job in the search results, click on the job name on the left, then click **Disable** on the right.

   Do this for all jobs. If the job is already disabled do nothing.

6. Run the following commands on LDAPHOST1:

   ```
   cd OUD_ORACLE_INSTANCE/OUD/bin
   ./ldapsearch -h ldaphost1 -p 1389 -D "cn=oudadmin" -b "" -s base
   "objectclass=*" lastExternalChangelogCookie

   Password for user 'cn=oudadmin': <OudAdminPwd>
   dn: lastExternalChangelogCookie:
   dc=mycompany,dc=com:00000140c682473c263600000862;
   ```

   Copy the output string that follows `lastExternalChangelogCookie:`. This value is required in the next step. For example,

   ```
   dc=mycompany,dc=com:00000140c682473c263600000862;
   ```

   The Hex portion must be 28 characters long. If this value has more than one Hex portion then separate the 28char portions with spaces. For example:

   ```
   dc=mycompany,dc=com:00000140c4ceb0c07a8d00000043 00000140c52bd0b9104200000042
   00000140c52bd0ba17b9000002ac 00000140c3b290b076040000012c;
   ```

7. Run each of the following LDAP reconciliation jobs once to reset the last change number.:

   - LDAP Role Delete Reconciliation
   - LDAP User Delete Reconciliation
   - LDAP Role Create and Update Reconciliation
   - LDAP User Create and Update Reconciliation
   - LDAP Role Hierarchy Reconciliation
   - LDAP Role Membership Reconciliation

   To run the jobs:

   a. Login to the OIM System Administration Console as the user `xelsysadm`.

   b. Under **System Management**, click **Scheduler**.

   c. Under **Search Scheduled Jobs**, enter `LDAP *` (there is a space before *) and hit **Enter**.

   d. Click on the job to be run.

   e. Set the parameter **Last Change Number** to the value obtained in step 6.

   For example:

   ```
   dc=mycompany,dc=com:00000140c4ceb0c07a8d00000043
   ```

```
00000140c52bd0b9104200000042 00000140c52bd0ba17b9000002ac
00000140c3b290b076040000012c;
```

f. Click **Run Now**.

g. Repeat for each of the jobs in the list at the beginning of this step.

8. For each incremental recon job whose last changelog number has been reset, execute the job and check that the job now completes successfully.

9. After the job runs successfully, re-enable periodic running of the jobs according to your requirements.

If the issue continues to occur, increase the cookie retention time to two months by running the following command on each OUD instance.

If, the error appears again after the incremental jobs have been re-enabled and run successfully ("Full resync required. Reason: The provided cookie is older..."), then increase the OUD cookie retention time. Although there is no hard and fast rule as to what this value should be, it should be long enough to avoid the issue, but small enough to avoid unnecessary resource consumption on OUD. One or two weeks should suffice; two week is given in the following example:

```
./dsconfig set-replication-server-prop --provider-name "Multimaster
Synchronization" --set replication-purge-delay:8w -D cn=oudadmin --trustAll -p
4444 -h LDAPHOST1

Password for user 'cn=oudadmin':  <OudAdminPswd>
Enter choice [f]: f
```

20.10.6 Troubleshooting Oracle SOA Suite

This section describes some common problems that can arise with Oracle SOA Suite and the actions you can take to resolve the problem. It contains the following topics:

20.10.6.1 Transaction Timeout Error

Problem: The following transaction timeout error appears in the log:

```
Internal Exception: java.sql.SQLException: Unexpected exception while enlisting
 XAConnection java.sql.SQLException: XA error: XAResource.XAER_NOTA start()
failed on resource 'SOADataSource_soaedg_domain': XAER_NOTA : The XID
is not valid
```

Solution: Check your transaction timeout settings, and be sure that the JTA transaction time out is less than the DataSource XA Transaction Timeout, which is less than the `distributed_lock_timeout` (at the database).

With the out of the box configuration, the SOA data sources do not set XA timeout to any value. The `Set XA Transaction Timeout` configuration parameter is unchecked in the WebLogic Server Administration Console. In this case, the data sources use the domain level JTA timeout which is set to `30`. Also, the default `distributed_lock_timeout` value for the database is `60`. As a result, the SOA configuration works correctly for any system where transactions are expected to have lower life expectancy than such values. Adjust these values according to the transaction times your specific operations are expected to take.

20.10.7 Troubleshooting Oracle Adaptive Access Manager

This section lists troubleshooting examples for Oracle Adaptive Access Manager.

20.10.7.1 Troubleshooting Session Accessed by Server that is not the Primary

Problem: You see errors in the log files similar to the following:

```
Warning: The session id: sessionID has been accessed from currentServer, a server
that is not the primary (primaryServer). The request URL was:requestUrl
```

The most likely cause is a configuration error on a front end hardware load balancer, or Web server plugin. They should be configured to recognize the values of primary/secondary in the cookie, for example, stickiness, when possible.

Solution: Ensure that the front end Web server or load balancer has been properly configured, particularly session stickiness.

A

Automation of the Process

This appendix describes how to write a scripts to invoke all of the scripts from a single host.

It is possible to write a script to invoke all of the scripts from a single host, in effect creating a one command deployment.

Below are sample scripts which can be modified to achieve this.

Disclaimer: These scripts are example implementations and are provided as is as a proof of concept to demonstrate a method to automate the deployment process. The scripts must be customized and tested for the specific need of your environment.

This appendix includes the following topics:

- Section A.1, "setenv.sh"
- Section A.2, "setlocalenv.sh"
- Section A.3, "deploy.sh"
- Section A.4, "Using the Scripts"
- Section A.5, "Troubleshooting"

A.1 setenv.sh

This script sets the environment.

```
#!/bin/sh
#
# setenv.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#     setenv.sh - captures details of environment to be deployed
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
#
#    NOTES
#      <other useful comments, qualifications, etc.>
#
#    MODIFIED   (MM/DD/YY)
```

```
#
CURRENT_HOST=`hostname`

export USERNAME=<unix user eg oracle>

export IDMTOP=SW_ROOT
export SHARED_CONFIG_DIR=$IDMTOP/config
export LOCAL_CONFIG_DIR=<LOCAL_ROOT>
export REPOSITORY=<REPOS_HOME>
export INSTALLERS=$REPOSITORY/installers
export RESPONSE_FILE=<FULLY QUALIFIED PATH TO DEPLOYMENT RESPONSE FILE>
export PROVISIONING=<IDMLCM_HOME>/provisioning
export SCRIPTS_DIR=<DIRECTORY CONTAINING THESE SCRIPTS>
export JAVA_HOME=$REPOSITORY/jdk6
export ANT_HOME=$REPOSITORY/provisioning/ant
export PRIMORDIAL_TO_DMZ_SHARE=$PROVISIONING/dmzShare

export RCU_ORACLE_HOME=$INSTALLERS/rcu
export RCU_LOG_LOCATION=$SCRIPTS_DIR/rcu/logs-$$
export RCU_LOG_NAME=rcu.log
export RCU_TIMESTAMP_LOG_DIR=false
export DB_SCHEMA_PREFIX=DEV

PHASES_TO_RUN='preverify install preconfigure configure configure-secondary
postconfigure startup validate'

export ALL_HOSTS='<LDAPHOST1> <LDAPHOST2> <OAMHOST1> <OAMHOST2> <OIMHOST1>
<OIMHOST2> <WEBHOST1> <WEBHOST2>'

export DB_CONNECT_STRING=<DB-SCAN>:<DB_LSNR_PORT>:<IDSTORE_SERVICE_NAME>
export DB_PASSWORD_SYS=<DB SYS PWD>
export DB_PASSWORD_SCHEMA=<RCU_SCHEMA_PASSWORD>

mkdir -p $PRIMORDIAL_TO_DMZ_SHARE

function timer()
{
    if [[ $# -eq 0 ]]; then
        echo $(date '+%s')
    else
        local  stime=$1
        etime=$(date '+%s')

        if [[ -z "$stime" ]]; then stime=$etime; fi
        dt=$((etime - stime))
        ds=$((dt % 60))
        dm=$(((dt / 60) % 60))
        dh=$((dt / 3600))
        printf '%d:%02d:%02d' $dh $dm $ds
    fi
}

 execCmd()
 {
   HOST=$1
   shift
   CMD_LINE=$*
   CMD="ssh $USERNAME@$HOST $CMD_LINE"

  echo "[idmprov] " `date` $CMD
  tmr=$(timer)
  $CMD

  printf '[idmprov] Elapsed time: %s\n' $(timer $tmr)
}
```

A.2 setlocalenv.sh

```
#!/bin/sh
#
# setlocalenv.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#     setenv.sh - captures details of environment to be deployed
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
#
#    NOTES
#      <other useful comments, qualifications, etc.>
#
#    MODIFIED   (MM/DD/YY)

#
CURRENT_HOST=`hostname`

export USERNAME=<software owner>

export IDMTOP=<SW_ROOT>
export SHARED_CONFIG_DIR=$IDMTOP/config
export LOCAL_CONFIG_DIR=<LOCAL_ROOT>
export REPOSITORY=<REPOS_HOME>
export INSTALLERS=$REPOSITORY/installers
export RESPONSE_FILE=<FULLY QUALIFIED PATH TO DEPLOYMENT RESPONSE FILE>
export PROVISIONING=<IDMLCM_HOME>/provisioning
export SCRIPTS_DIR=<DIRECTORY CONTAINING THESE SCRIPTS>
export JAVA_HOME=$REPOSITORY/jdk6
export ANT_HOME=$REPOSITORY/provisioning/ant
export PRIMORDIAL_TO_DMZ_SHARE=$PROVISIONING/dmzShare
```

A.3 deploy.sh

This is the Deployment script.

```
#!/bin/sh
#
# deploy.sh
#
# Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.
#
#    NAME
#      provision.sh - this script starts executing Deployment phases in all hosts
#
#    DESCRIPTION
#      <short description of component this file declares/defines>
```

```
#
#    NOTES
#      - copy all scripts named prov_*.sh to a directory in primordial host
#      - make sure this directory is accessible using the same path from all hosts
being provisioned
#      - update prov_env.sh with environment specific details (directories,
hostnames, db, etc)
#      - run this script from the primordial host
#      - script will create one log file for each phase in each host - named prov_
run-<phase>-<host>.log
#      - script will stop when Deployment completes or on detecting 1st failure
(absence of "BUILD SUCCESSFUL" in the log file)
#
#    MODIFIED   (MM/DD/YY)
#

. <DIRECTORY CONTAINING THESE SCRIPTS>/setenv.sh

if [ ! -e $SCRIPTS_DIR/logs ]
then
     mkdir -p $SCRIPTS_DIR/logs
fi

rm -r $SCRIPTS_DIR/logs/* LCM_ROOT/provisioning* <LCM_ROOT>/internal LCM_
ROOT/lcmconfig LCM_ROOT/keystores 2> /dev/null

starttmr=$(timer)

for PHASE in $PHASES_TO_RUN
do
  phasetmr=$(timer)
  for HOST in $ALL_HOSTS
  do
    echo "[idmprov] Running $PHASE on  $HOST"
    logFile=$SCRIPTS_DIR/logs/$PHASE-$HOST.log

    execCmd $HOST ". $SCRIPTS_DIR/setlocalenv.sh; cd $PROVISIONING/bin;
./runIAMDeployment.sh -responseFile $RESPONSE_FILE -target $PHASE" > $logFile

    fgrep -s "BUILD SUCCESSFUL" $logFile
    if [ "$?" = "1" ]
    then
        echo "ERROR: $PHASE failed in $HOST"
        exit 1
    fi

  done

  echo -e "[idmprov] Total $PHASE\c"
  printf ' time: %s\n' $(timer $phasetmr)
done

printf '[idmprov] Total Elapsed time: %s\n' $(timer $starttmr)
```

A.4 Using the Scripts

Use the scripts as follows:

1. Copy the scripts to a location that is available on each host in the topology.

2. Edit the scripts and replace entries like <SW_ROOT> with entries applicable to your environment. Use Section 11.1, "Assembling Information for Identity and Access Management Deployment," to assist with this.
3. Set up ssh equivalence from the primordial host to each of the other hosts in the topology. See your operating system documentation for details.
4. Validate that ssh equivalence is working by issuing the following command from the primordial host to each host in the topology. This command should show the date on each remote machine without any prompts:

   ```
   ssh hostname date
   ```

5. Copy the deployment response file generated in Chapter 13, "Creating a Deployment Profile," to the same directory where these scripts are located.
6. Run the deploy.sh script.
7. After deployment is complete, remove the ssh equivalence.

A.5 Troubleshooting

Problem

Preverify fails on Exalogic host with the error: Invalid OS.

Solution

This occurs because the operating system name is slightly different from the name listed in idm-common-preverify-build.xml. To fix this problem, edit the file so that the value of the entry:

```
<property name="oracle.prov.validate.os.versions3"
```

includes the string:

```
Enterprise Linux Server release 5.*]
```

B

Cleaning Up an Environment Before Rerunning IAM Deployment

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

When you provision Oracle Identity and Access Management using the `runIAMDeployment.sh` command, you must complete each stage in the topology before beginning the next stage, in a specified order. If a stage fails, you must clean up and start over.

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

1. On each host, stop all Identity and Access Management processes. To do this, you should restart the host.
2. On each host, remove the contents of the directory *`LOCAL_ROOT`*.

   Note: Exclude this step for an Oracle Traffic Director installation.

3. Remove the contents of the directory IDM_TOP on shared storage.

   Note: Leave the *OTD_ORACLE_HOME* directory intact.

   Note: In this example, *SHARED_CONFIG_DIR* is nested under *IDM_TOP*. As a result, it is also deleted. However, if you have *SHARED_CONFIG_DIR* in a different location, delete it explicitly as well.

4. Remove the contents of the *LCM_HOME*`/provisioning` directory.
5. Using the Repository Creation Utility, drop all schemas created in Section 10.5, "Loading the Identity and Access Management Schemas in the Oracle RAC Database by Using RCU."

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

C

Topology Tool Commands for Scaling

This appendix describes useful `topotool.sh` commands for scaling an Identity and Access Management enterprise deployment.

During deployment, a topology store is created which contains details of the deployed topology. When patching the environment, the Lifecycle Tools read the store in order to build and execute the patch plan.

Chapter 19, "Scaling Enterprise Deployments" describes how to scale the deployment up or out using a variety of tools. As part of a scaling procedure, you must add new entries to the store covering the new additions to the deployment. This is done using the IAM Topology Tool.

The tool is located at: *`IDMLCM_HOME`*`/topotool/bin`

Before running the Topology Tool, back up your entire *`LCM_ROOT`*`/lcmconfig/topology` directory.

> **Note:** Many of the command-line options use instance or component names that include numbers, for example `OUD3`. You should already have determined these names when you assembled information for scaling. See the Assembling Information sections in Chapter 19, "Scaling Enterprise Deployments."

This chapter contains the following sections:

- Section C.1, "Syntax of the Topology Tool"
- Section C.2, "Commonly-Used Command Line Operations"
- Section C.3, "Steps and Command-Line Examples"

C.1 Syntax of the Topology Tool

The general syntax is:

```
topotool.sh command [-option]
```

For help, use:

```
topotool.sh [-help]

topotool.sh command [-help]
```

Note: This section is not a complete description of the syntax of the Topology Tool. The commands and options listed in this section include only those that are used in this guide.

C.1.1 Commands

Add

Adds information to the topology store.

```
topotool.sh add [options]
```

Modify

Modifies information in the topology store.

```
topotool.sh modify [options]
```

C.1.2 Command-Line Options Used with Add

-component

Specifies adding of a component.

-confighomename oud*n* | oim*n* | oam*n* | soa*n* | NodeManager:Access | NodeManager:Identity | ohs*n*

Specifies a local or shared configuration home to add. Used with `-instance`.

-dbname *DBNAME*

Specifies the Oracle Database to use. Used with `-instance`. In this guide, *`DBNAME`* is always `OIM:DB`.

-description *STRING*

Used with `-machine` and `-confighome`. *`STRING`* is a quoted string, such as `"oim3 machine"`.

-fqdn *HOSTNAME*

Specifies a host. The *`HOSTNAME`* format is a fully qualified domain name, such as `ldaphost3.mycompany.com`, `oimhost4.mycompany.com`. Used with `-host`.

-hometype OUD | IAM | SOA | WEBTIER

Specifies the home type to be added. Used with `-instance`.

-host

Specifies adding a host.

-instance

Specifies adding an instance.

-instancegroup *STRING*

Specifies an instance group. In this guide, `STRING` is always `1` when used with `-instancegroup`. Used with `-instance`.

-machine

Specifies adding a machine

-machinename *MACHINE*

Specifies the machine to be added. Used with `-instance` and `-machine`. The format of `MACHINE` is a fully qualified machine name such as `ldaphost3.mycompany.com`, `oimhost4.mycompany.com`.

-mwhomename Directorytier:MW_HOME | Access:MW_HOME | Identity:MW_HOME | Webtier:MW_HOME | Webtier:MW_HOME_2 | Webtier:MW_HOME_*n*

Specifies the Middleware home to add. Used with `-instance`

-name *NAME*

Specifies the name of a machine or an instance. When used with `-machine`, the *NAME* format is a fully-qualified hostname, such as `ldaphost3.mycompany.com`.

When used with `-instance` or `-confighome`, the *NAME* format is `productn`, for example `oid3`.

When used with `-instance`, the *NAME* format is a hostname and port pair, in the format `productn:host:plain` for a non-SSL port and `productn:host:ssl` for an SSL port, where `product` is a component, such as `OUD` or `OIM`, and `n` is the instance number.

When used to add an OPMN instance the hostname part of the *NAME* format is `OPMN`, for example: `OPMN:webhost3:ssl`.

-path *PATH*

Specifies a quoted directory path, such as `"/u01/oracle/config/nodemanager/oimhost3.mycompany.com"`. Used with `-confighome`

-port *PORT*

Specifies a port number, such as 5556. Used with `-host`.

-secure true | false

Set to `true` for an SSL port and `false` for a non-SSL port. Used with `-host`.

-shared true | false

used with `-confighome` to indicate whether this is a shared or local configuration home.

-sharedlcmconfigaccessible true | false

Specifies whether the shared LCM configuration is accessible. Used with `-machine`. In this guide, it is set to `true` when adding application tier machines and to `false` for web tier machines.

-tier DIRECTORY | IDM | WEB |

Specifies the tier, as listed in Chapter 19, "Scaling Enterprise Deployments."

-type TYPE

Specifies the type of an instance or a component. In both cases, **TYPE** stands for the specific type definition to be used, matching the instance or component being added.

When used with `-instance`, the value can be one of: OUD | OHS_HTTPD | OPMN WLS_ADMIN | WLS_MANAGED | WLS_NODE_MANAGER

When used with `-component`, the value can be one of: OHS_WEBGATE | WLS_ADMIN_OAM_CONSOLE | WLS_ADMIN_WLS_CONSOLE | WLS_MANAGED_OAM | WLS_MANAGED_OIM | WLS_MANAGED_SOA

-virtual true | false

Specifies whether the host being added is a virtual host. Used with `-host`. It is always `false` in this guide.

C.1.3 Command-Line Options Used with Modify for Updating Load Balancer Mappings

-lbrmapping

Specifies modification of the load balancer mapping by the addition of a new host

-lbrname *LBRNAME*

Used with `-lbrmapping`. Specifies the name of the load balancer. *`LBRNAME`* is always `LBR1` or `LBR2` in this guide.

-name idstore | idstore_ssl

Used with `-lbrmapping`. Specifies the load balancer mapping name.

-physicalhosts *HOSTS*

Used with `-lbrmapping`. Specifies a host or a comma-separated list of hosts. For a non-SSL host, the format is *`productn`*`:`*`host`*, for example: `OUD:LDAP:oud1:ldaphost1,oud2:ldaphost2,oud3:ldaphost3`. For an SSL host, the format is *`productn`*`:`*`host`*`:ssl`, for example: oud3:ldaphost3:ssl

C.2 Commonly-Used Command Line Operations

Adding a Machine:

```
topotool.sh add -machine -name MACHINE -sharedlcmconfigaccessible true_false
```

Adding a Non-SSL Host:

```
topotool.sh add -host -name HOST -fqdn FQDN -port PORT -secure false -virtual
false
```

Adding an SSL Host:

```
topotool.sh add -host -name HOST_SSL -fqdn FQDN -port SSL_PORT -secure false
-virtual false
```

Adding a Local Configuration Home:

```
topotool.sh add -confighome -name LOCAL_CONFIG -path PATH -shared false
```

Adding a Shared Configuration Home:

```
topotool.sh add -confighome -name SHARED_CONFIG -path
"/u01/oracle/config/instances/oud3" -shared true
```

Adding an Instance:

```
topotool.sh add -instance -machinename MACHINE -name INSTANCE -type TYPE -tier
TIER -mwhomename MWHOME-hometype  -confighomename  LOCAL_OR_SHARED_CONFIG
-instancegroup 1
```

Adding a Component:

```
topotool.sh add -component -instancename INSTANCE -type TYPE -hosts HOST
```

Updating LBR Mappings:

```
topotool.sh modify -lbrmapping -lbrname LBR -name LBR_MAPPING -physicalhosts HOST
topotool.sh modify -lbrmapping -lbrname LBR_SSL -name LBR_MAPPING -physicalhosts
HOST_SSL
```

C.3 Steps and Command-Line Examples

This section contains notes about each tier, general steps for scaling out the components in that tier, and example command lines. It contains the following topics:

- Section C.3.1, "Scaling Out / Scaling Up of Directory Tier"
- Section C.3.2, "Scaling Out / Scaling Up of Application Tier"
- Section C.3.3, "Scaling Out / Scaling Up of Web Tier"

> **Note:** Do not use the examples directly. You must substitute the values with your own data.

C.3.1 Scaling Out / Scaling Up of Directory Tier

The following sections provide information about scaling the directory tier.

- Section C.3.1.1, "Directory Tier Notes"
- Section C.3.1.2, "Topology Tool Steps for Scaling Oracle Unified Directory"
- Section C.3.1.3, "Scale Out Commands for Oracle Unified Directory"
- Section C.3.1.4, "Scale Up Commands for Oracle Unified Directory"

C.3.1.1 Directory Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the LDAP hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.
- Reconfigure load balancer mappings.

C.3.1.2 Topology Tool Steps for Scaling Oracle Unified Directory

1. Add a machine with `sharedlcmconfigaccessible` set to true. (Only for scale out).
2. Add a non-SSL host if Oracle Unified Directory is listening on non-SSL port.
3. Add a SSL host if Oracle Unified Directory is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type OUD, tier DIRECTORY, hometype OUD using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Update the load balancer mappings with the newly created non-SSL or SSL hosts.

C.3.1.3 Scale Out Commands for Oracle Unified Directory

- Adding new machine

  ```
  topotool.sh add -machine -name ldaphost3.mycompany.com -description "oud3
  machine" -sharedlcmconfigaccessible true
  ```

- Adding new host (hostname + port combination)
  - Non-SSL:

    ```
    topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.mycompany.com
    -port 1389 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn
    ldaphost3.mycompany.com -port 1390 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oud3 -description "oud3 local
    configuration home" -path "/u02/private/oracle/config/instances/oud3"
    -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oud3 -description "oud3 configuration
    home" -path "/u01/oracle/config/instances/oud3" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename ldaphost3.mycompany.com -name oud3
  -description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
  HOME -hometype OUD -confighomename oud3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
  oud3:ldaphost3,oud3:ldaphost3:ssl
  ```

- Adding the new host to the load balancer mappings
  - Non-SSL:

    ```
    topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
    ```

```
oud3:ldaphost3
```

- SSL:

  ```
  topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
  -physicalhosts oud3:ldaphost3:ssl
  ```

C.3.1.4 Scale Up Commands for Oracle Unified Directory

- Adding new machine

  ```
  topotool.sh add -machine -name ldaphost3.mycompany.com -description "oud3
  machine" -sharedlcmconfigaccessible true
  ```

- Adding new host (hostname + port combination)

  - Non-SSL:

    ```
    topotool.sh add -host -name oud3:ldaphost3 -fqdn ldaphost3.mycompany.com
    -port 1389 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oud3: ldaphost3:ssl -fqdn
    ldaphost3.mycompany.com -port 1390 -secure true -virtual false
    ```

- Adding new config home

  - Local config:

    ```
    topotool.sh add -confighome -name oud3 -description "oud3 local
    configuration home" -path "/u02/private/oracle/config/instances/oud3"
    -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oud3 -description "oud3 configuration
    home" -path "/u01/oracle/config/instances/oud3" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename ldaphost3.mycompany.com -name oud3
  -description "oud3" -type OUD -tier DIRECTORY -mwhomename Directorytier:DIR_MW_
  HOME -hometype OUD -confighomename oud3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oud3 -type DEFAULT  -hosts
  oud3:ldaphost3,oud3:ldaphost3:ssl
  ```

- Adding the new host to the load balancer mappings

  - Non-SSL:

    ```
    topotool.sh modify -lbrmapping -lbrname LBR2 -name idstore -physicalhosts
    oud3:ldaphost3
    ```

  - SSL:

    ```
    topotool.sh  modify -lbrmapping -lbrname LBR2 -name idstore-ssl
    -physicalhosts oud3:ldaphost3:ssl
    ```

C.3.2 Scaling Out / Scaling Up of Application Tier

The following sections provide information about scaling the application tier.

- Section C.3.2.1, "Application Tier Notes"
- Section C.3.2.2, "Topology Tool Steps for OAM"
- Section C.3.2.3, "Scale Out Commands for OAM"
- Section C.3.2.4, "Scale Up Commands for OAM"
- Section C.3.2.5, "Topology Tool Steps for OIM"
- Section C.3.2.6, "Scale Out commands for OIM"
- Section C.3.2.7, "Scale Up commands for OIM"
- Section C.3.2.8, "Topology Tool Steps for SOA"
- Section C.3.2.9, "Scale Out commands for SOA"
- Section C.3.2.10, "Scale Up Commands for SOA"

C.3.2.1 Application Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries are shared among the hosts.
- When scaling out, the shared binary directory is mounted onto the new host.
- The shared config directory is also mounted onto the new host.
- Node manager added in case of Scale Out.

C.3.2.2 Topology Tool Steps for OAM

1. Add a machine with `sharedlcmconfigaccessible` set to `true`. (Only for scale out).
2. Add a non-SSL host if OAM is listening on non-SSL port.
3. Add a SSL host if OAM is listening on SSL port.
4. Add a host for OAP.
5. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
6. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
7. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
8. Add a component for the newly created instance of type WLS_MANAGED_OAM using the newly created non-SSL or SSL hosts.

C.3.2.3 Scale Out Commands for OAM

- Adding new machine

  ```
  topotool.sh add -machine -name oamhost3.mycompany.com -description "oam3
  machine" -sharedlcmconfigaccessible true
  ```

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

```
topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.mycompany.com
-port 14100 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.mycompany.com
-port 14101 -secure true -virtual false
```

- Adding the new host for OAP (hostname + port combination)

```
topotool.sh add -host -name oam3:slc03oap3 -fqdn oamhost3.mycompany.com -port
5575 -secure false -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oam3 -description "oam3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oam3 -description "oam3 shared
configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.mycompany.com -name oam3
-description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
-hometype IAM -confighomename oam3 -dbname OIM:DB -domainname   IAMAccessDomain
-instancegroup 1
```

- Adding new component

```
topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
oam3:oamhost3,oam3:oamhost3:ssl
```

C.3.2.4 Scale Up Commands for OAM

- Adding new host (hostname + port combination) for OAM
  - Non-SSL:

```
topotool.sh add -host -name oam3:oamhost3 -fqdn oamhost3.mycompany.com
-port 14100 -secure false -virtual false
```

  - SSL:

```
topotool.sh add -host -name oam3:oamhost3:ssl -fqdn oamhost3.mycompany.com
-port 14101 -secure true -virtual false
```

- Adding new config home
  - Local config:

```
topotool.sh add -confighome -name oam3 -description "oam3 local
configuration home" -path
"/u02/private/oracle/config/domains/IAMAccessDomain" -shared false
```

  - Shared config:

```
topotool.sh add -confighome -name oam3 -description "oam3 shared
configuration home" -path "/u01/oracle/config/domains/IAMAccessDomain/"
-shared true
```

- Adding new instance

```
topotool.sh add -instance -machinename oamhost3.mycompany.com -name oam3
-description "oam3" -type WLS_MANAGED -tier IDM -mwhomename Access:IAD_MW_HOME
-hometype IAM -confighomename oam3 -dbname OIM:DB -domainname   IAMAccessDomain
-instancegroup 1
```

- Adding component

```
topotool.sh add -component -instancename oam3 -type WLS_MANAGED_OAM  -hosts
oam3:oamhost3, oam3:oamhost3:ssl,oam3:slc03oap3

topotool.sh add -component -instancename oam3 -type DEFAULT  -hosts
oam3:oamhost3,oam3:oamhost3:ssl
```

C.3.2.5 Topology Tool Steps for OIM

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if OIM is listening on non-SSL port.
3. Add a SSL host if OIM is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype IAM using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_OIM using the newly created non-SSL or SSL hosts.

C.3.2.6 Scale Out commands for OIM

- Adding new machine

```
topotool.sh add -machine -name oimhost3.mycompany.com -description "oim3
machine" -sharedlcmconfigaccessible true
```

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.mycompany.com
    -port 14000 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.mycompany.com
    -port 14001 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 local
    configuration home" -path
    ```

```
"/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
```

  - Shared config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name oim3
  -description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
  oim3:oimhost3,oim3:oimhost3:ssl

  topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
  oim3:oimhost3,oim3:oimhost3:ssl
  ```

C.3.2.7 Scale Up commands for OIM

- Adding new host (hostname + port combination) for OIM
  - Non-SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3 -fqdn oimhost3.mycompany.com
    -port 14000 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name oim3:oimhost3:ssl -fqdn oimhost3.mycompany.com
    -port 14001 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name oim3 -description "oim3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name oim3
  -description "oim3" -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype IAM -confighomename oim3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename oim3 -type WLS_MANAGED_OIM -hosts
  oim3:oimhost3,oim3:oimhost3:ssl
  ```

```
topotool.sh add -component -instancename oim3 -type DEFAULT -hosts
oim3:oimhost3,oim3:oimhost3:ssl
```

C.3.2.8 Topology Tool Steps for SOA

1. Add a machine with sharedlcmconfigaccessible set to true. (Only for scale out).
2. Add a non-SSL host if SOA is listening on non-SSL port.
3. Add a SSL host if SOA is listening on SSL port.
4. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
5. Add an instance of type WLS_MANAGED, tier IDM, hometype SOA using an existing middleware home.
6. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
7. Add a component for the newly created instance of type WLS_MANAGED_SOA using the newly created non-SSL or SSL hosts.

C.3.2.9 Scale Out commands for SOA

- Adding new machine

  ```
  topotool.sh add -machine -name oimhost3.mycompany.com -description "soa3
  instance machine" -sharedlcmconfigaccessible true
  ```

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.mycompany.com
    -port 8001 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.mycompany.com
    -port 8002 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name soa3
  -description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

```
topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
soa3:oimhost3,soa3:oimhost3:ssl

topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
soa3:oimhost3,soa3:oimhost3:ssl
```

C.3.2.10 Scale Up Commands for SOA

- Adding new host (hostname + port combination) for SOA
  - Non-SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3 -fqdn oimhost3.mycompany.com
    -port 8001 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name soa3:oimhost3:ssl -fqdn oimhost3.mycompany.com
    -port 8002 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 local
    configuration home" -path
    "/u02/private/oracle/config/domains/IAMGovernanceDomain" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name soa3 -description "soa3 shared
    configuration home" -path "
    /u01/oracle/config/domains/IAMGovernanceDomain"-shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name soa3
  -description "soa3 " -type WLS_MANAGED -tier IDM -mwhomename Identity::IGD_MW_
  HOME -hometype SOA -confighomename soa3 -dbname OIM:DB -domainname
  IAMGovernanceDomain -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename soa3 -type WLS_MANAGED_SOA -hosts
  soa3:oimhost3,soa3:oimhost3:ssl

  topotool.sh add -component -instancename soa3 -type DEFAULT -hosts
  soa3:oimhost3,soa3:oimhost3:ssl
  ```

C.3.2.11 Steps for Adding Node Manager Steps for OAM/OIM/SOA Scale Out Only

1. Add a non-SSL host if Node Manager is listening on non-SSL port.
2. Add a SSL host if Node Manager is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
4. Add an instance of type WLS_NODE_MANAGER, tier IDM, hometype IAM using an existing middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.

6. Add a component for the newly created instance of type WLS_NODE_MANAGER using the newly created non-SSL or SSL hosts.

C.3.2.12 Commands for Adding NodeManager for Scale Out of OAM

- Adding new host (hostname + port combination) for Node Manager OAM
  - Non-SSL:

    ```
    topotool.sh add -host -name NodeManager:oamhost3 -fqdn
    oamhost3.mycompany.com -port 5556 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name NodeManager:oamhost3:ssl -fqdn
    oamhost3.mycompany.com -port 5556 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name NodeManager:Access -description "node
    manager local configuration home" -path
    "/u01/oracle/config/nodemanager/oamhost3.mycompany.com" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name NodeManager:Access -description " node
    manager shared configuration home " -path
    "/u01/oracle/config/nodemanager/oamhost3.mycompany.com" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oamhost3.mycompany.com -name
  NodeManager:Access -description "node manager  instance" -type WLS_NODE_MANAGER
  -tier IDM -mwhomename Access:IAD_MW_HOME -hometype IAM -confighomename
  NodeManager:Access  -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename NodeManager:Access -type DEFAULT
  -hosts NodeManager:oamhost3, NodeManager:oamhost3:ssl
  ```

C.3.2.13 Commands for Adding NodeManager for Scale Out of OIM

- Adding new host (hostname + port combination) for Node Manager OIM
  - Non-SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3 -fqdn
    oimhost3.mycompany.com -port 5556-secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
    oimhost3.mycompany.com -port 5556 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name NodeManager:Identity -description "node
    manager local configuration home" -path
    "/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name NodeManager:Identity -description " node
    manager shared configuration home " -path
    "/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name
  NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
  MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
  -confighomename NodeManager:Identity  -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
  -hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
  ```

C.3.2.14 Commands for Adding NodeManager for Scale Out of SOA

- Adding new host (hostname + port combination) for Node Manager SOA
  - Non-SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3 -fqdn
    oimhost3.mycompany.com -port 5556-secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name NodeManager:oimhost3:ssl -fqdn
    oimhost3.mycompany.com -port 5556 -secure true -virtual false
    ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name NodeManager:Identity -description "node
    manager local configuration home" -path
    "/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name NodeManager:Identity -description " node
    manager shared configuration home " -path
    "/u01/oracle/config/nodemanager/oimhost3.mycompany.com" -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename oimhost3.mycompany.com -name
  NodeManager:Identity -description "node manager  instance" -type WLS_NODE_
  MANAGER -tier IDM -mwhomename Identity::IGD_MW_HOME -hometype IAM
  -confighomename NodeManager:Identity  -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename NodeManager:Identity -type DEFAULT
  -hosts NodeManager:oimhost3, NodeManager:oimhost3:ssl
  ```

C.3.3 Scaling Out / Scaling Up of Web Tier

The following sections provide information about scaling the web tier.

C.3.3.1 Web Tier Notes

- Scale Out and Scale Up supported.
- Oracle Binaries not shared. They are local.
- The config directory is not mounted.
- Reconfigure Load Balancer.

C.3.3.2 Topology Tool Steps for Scaling OHS

1. Add a machine with sharedlcmconfigaccessible set to false. (Only for scale out).
2. Add a non-SSL host if OHS is listening on non-SSL port.
3. Add a SSL host if OHS is listening on SSL port.
4. Add a new Middleware Home with shared set as false. (Only for scale out)
5. Add a new Oracle Home. (Only for scale out)
6. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
7. Add an instance of type OHS_HTTPD, tier WEB, hometype WEBTIER using the newly created middleware home or existing middleware home in case of scale up.
8. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.
9. Add a component for the newly created instance of type OHS_WEBGATE using the newly created non-SSL or SSL hosts.
10. Update the SSO, IDMINTERNAL, OIMADMIN, OAMADMIN load balancer mappings with the newly created non-SSL or SSL hosts.

C.3.3.3 Scale Out Commands for Web

- Adding new machine

  ```
  topotool.sh add -machine -name webhost3.mycompany.com -description "ohs3
  machine" -sharedlcmconfigaccessible false
  ```

- Adding new host (hostname + port combination)
  - Non-SSL:

    ```
    topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.mycompany.com
    -port 7777 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.mycompany.com
    -port 7778 -secure true -virtual false
    ```

- Adding new MW Home(s)

  ```
  topotool.sh add -mwhome -name Webtier:WEB_MW_HOME -path
  /u01/oracle/products/ohs/ -shared false
  ```

- Adding new Oracle Home(s)

  ```
  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type ORACLE_COMMON -path
  /u01/oracle/products/ohs/oracle_common

  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type WEBTIER -path
  /u01/oracle/products/ohs/ohs

  topotool.sh add -home -mwhomename Webtier:WEB_MW_HOME -type OAM_WG -path
  /u01/oracle/products/ohs/webgate
  ```

- Adding new config home
  - Local config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 local
    configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
    -shared false
    ```

  - Shared config:

    ```
    topotool.sh add -confighome -name ohs3 -description "ohs3 shared
    configuration home" -path " /u02/private/oracle/config/instances/ohs3"
    -shared true
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name ohs3
  -description "ohs3 instance" -type OHS_HTTPD -tier WEB -mwhomename Webtier:WEB_
  MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
  ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

  topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
  ohs3:webhost3,ohs3:webhost3:ssl
  ```

- Adding the new host to the load balancer mappings
  - Adding to sso LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to idminternal LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name idminternal
    -physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oimadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

  - Adding to oamadmin LBR mapping

    ```
    topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
    ohs3:webhost3,ohs3:webhost3:ssl
    ```

C.3.3.4 Scale Up Commands for OHS

- Adding new host (hostname + port combination)
    - Non-SSL:

      ```
      topotool.sh add -host -name ohs3:webhost3 -fqdn webhost3.mycompany.com
      -port 7777 -secure false -virtual false
      ```

    - SSL:

      ```
      topotool.sh add -host -name ohs3:webhost3:ssl -fqdn webhost3.mycompany.com
      -port 7778 -secure true -virtual false
      ```

- Adding new config home
    - Local config:

      ```
      topotool.sh add -confighome -name ohs3 -description "ohs3 local
      configuration home" -path " /u02/private/oracle/config/instances/ohs1 "
      -shared false
      ```

    - Shared config:

      ```
      topotool.sh add -confighome -name ohs3 -description "ohs3 shared
      configuration home" -path " /u02/private/oracle/config/instances/ohs3"
      -shared true
      ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name ohs3
  -description "ohs3" -type OHS_HTTPD -tier WEB -mwhomename Webtier:MW_HOME
  -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename ohs3 -type OHS_WEBGATE -hosts
  ohs3:webhost3,ohs3:webhost3:ssl -clienthosts oam3:slc03oap3

  topotool.sh add -component -instancename ohs3 -type DEFAULT -hosts
  ohs3:webhost3,ohs3:webhost3:ssl
  ```

- Adding the new host to the load balancer mappings
    - Adding to sso LBR Mapping

      ```
      topotool.sh modify -lbrmapping -lbrname LBR1 -name sso  -physicalhosts
      ohs3:webhost3,ohs3:webhost3:ssl
      ```

    - Adding to idminternal LBR mapping

      ```
      topotool.sh modify -lbrmapping -lbrname LBR1 -name idminternal
      -physicalhosts ohs3:webhost3,ohs3:webhost3:ssl
      ```

    - Adding to oimadmin LBR mapping

      ```
      topotool.sh modify -lbrmapping -lbrname LBR1 -name oimadmin -physicalhosts
      ohs3:webhost3,ohs3:webhost3:ssl
      ```

    - Adding to oamadmin LBR mapping

      ```
      topotool.sh modify -lbrmapping -lbrname LBR1 -name oamadmin -physicalhosts
      ohs3:webhost3,ohs3:webhost3:ssl
      ```

C.3.3.5 Steps for Adding OPMN for Webtier Scale Up and Scale Out

1. Add a non-SSL host if OPMN is listening on non-SSL port.
2. Add a SSL host if OPMN is listening on SSL port.
3. Add a configuration home. Set shared to true / false based on whether it is shared configuration or local configuration.
4. Add an instance of type OPMN, tier WEB, hometype WEBTIER using an existing web tier middleware home.
5. Add a component for the newly created instance of type DEFAULT using the newly created non-SSL or SSL hosts.

C.3.3.6 Commands for Adding OPMN Instance for WEB Tier for Scale Out and Scale Up

- Adding new host (hostname + port combination)
  - Non-SSL:

    ```
    topotool.sh add -host -name OPMN:ohs3 -fqdn webhost3.mycompany.com -port
    6700 -secure false -virtual false
    ```

  - SSL:

    ```
    topotool.sh add -host -name OPMN:webhost3:ssl -fqdn webhost3.mycompany.com
    -port 6701 -secure true -virtual false
    ```

- Adding new instance

  ```
  topotool.sh add -instance -machinename webhost3.mycompany.com -name OPMN:ohs3
  -description "opmn for ohs third instance" -type OPMN -tier WEB -mwhomename
  Webtier:MW_HOME -hometype WEBTIER -confighomename ohs3 -instancegroup 1
  ```

- Adding new component

  ```
  topotool.sh add -component -instancename OPMN:ohs3 -type DEFAULT -hosts
  OPMN:webhost3, OPMN:webhost3:ssl
  ```

D

Configuring External Access to an Internal Exalogic IAM Deployment

This chapter describes how to configure an Exalogic Identity and Access Management deployment so that it can communicate with applications outside of the Exalogic rack.

If you have configured your Exalogic Identity and Access Management deployment to use the internal network of the Exalogic machine, then you have configured a fully functioning deployment for all applications that are deployed within the Exalogic rack. This configuration, however, does not enable you to protect applications outside of the Exalogic rack, because the security agents cannot talk to the Oracle Access Management Access Manager servers, which are only available on the internal Exalogic network.

In order to achieve a deployment where you have an external agent such as Oracle WebGate protecting a third party application such as SOA or Web Center, you must enable the external agent to communicate with the OAM servers using the public access network. To do this you need to perform the following additional steps.

First, ensure that your Exalogic Compute Nodes or vServers have access to the external Client Access Network using EoIB.

By default, your configuration is configured so that SSO agents communicate with the Access Manager servers, identified as host names iamhost1 and iamhost2, using the internal network.

In summary the steps you must perform are:

1. Create Access Manager server instances registered using the client access network names for those servers.
2. Create an SSO agent inside Access Manager which uses the external Access Manager servers.
3. Configure the external WebGate to use the external SSO agent.

The example in this appendix shows how to protect a simple HTML test page on an external OHS using web gate. It includes the following sections:

- Section D.1, "Creating New OAM Server Instances Listening on the External Network"
- Section D.2, "Creating a New SSO Agent"
- Section D.3, "Creating a Test Resource in OAM"
- Section D.4, "Configuring the External Oracle HTTP Server"
- Section D.5, "Validating the Installation"

D.1 Creating New OAM Server Instances Listening on the External Network

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad, click **Server Instances**.
3. When the search window is displayed, click **Search**.

   You will see your existing server instances displayed: wls_oam1 and wls_oam2.
4. Create two new server instances by clicking the **Create** button and entering the appropriate information. This example shows the values for wls_oam1_ext:
   - **Server Name**: `wls_oam1_ext`
   - **Host**: `iamhost1ext.mycompany.com` (Use the name associated with the client access network.)
   - **Port**: `14000` (*`OIM_PORT`*)
   - **Proxy Server Id**: `AccessServerConfigProxy`
   - **Proxy Port**: `5575` (*`OAM_PROXY_PORT`*)
   - **Mode**: `Simple`

   Leave all other values as they are and click **Apply**.
5. Repeat for Server Name wls_oam2-ext.

You now have four Access Manager server instances, two listening on the internal network and two listening on the external network.

D.2 Creating a New SSO Agent

You can use either `rreg` or the OAM console to create a new SSO Agent. For the purposes of this example we will create a new SSO Agent using the console and using the existing Application Domain IAMSuiteAgent, but for your applications how you create the agent will be dependent on the application you are protecting. Refer to your product documentation for details.

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad, click **SSO Agents**.
3. Click **Create 11g Webgate**.
4. Create with the same values as the existing agent Webgate_IDM_11g, except for these three values:
   - **Name for Example**: `Webgate_External`
   - Deselect **Auto Create Policies**.
   - **Host Identifier** `IAMSuiteAgent`
5. Click **Apply a new web gate agent called Webgate_External**.
6. Edit the newly created agent by clicking **SSO Agents** from the Launch Pad.
7. Click **Search**.
8. Click on the newly created agent **Webgate_External**.

9. Remove all servers from the Primary Server list other than wls_oam1-ext and wls_oam2-ext
10. Click **Apply**.

D.3 Creating a Test Resource in OAM

1. Log in to the OAM Console for IAMAccessDomain at the URL listed in Section 20.2, "About Identity and Access Management Console URLs."
2. From the Launch Pad click **Application Domains**.
3. When the Search Application Domains Window is displayed, click **Search**.
4. Click on the **Application Domain IAM Suite Agent**.
5. Click **Resources** tab.
6. Click **New Resource** and enter the following information:
   - **Type**: `Http`
   - **Description**: `Test Resource`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/sso.html`
   - **Protection Level**: `Protected`
   - **Authentication Policy**: `Protected Higher Level Policy`
   - **Authorization Policy**: `Protected Resource Policy`
7. Click **Apply**.

D.4 Configuring the External Oracle HTTP Server

Install and configure Oracle HTTP server on your external server.

Create a test HTML page called `sso.html` and place it in the OHS `htdocs` folder.

Install WebGate on your external server.

Deploy WebGate to Oracle HTTP, as follows:

1. Execute the command `deployWebGateInstance.sh` which is located in:

   ```
   WEBGATE_ORACLE_HOME/webgate/ohs/tools/deployWebGate
   ```

   The command takes the following arguments:

   - Oracle HTTP instance configuration directory
   - WebGate home directory

   For example:

   ```
   ./deployWebGateInstance.sh -w WEB_ORACLE_INSTANCE/config/OHS/component_name -oh
   WEBGATE_ORACLE_HOME
   ```

2. Set the library path.

   For example, set the library path to include the *`WEB_ORACLE_HOME`*`/lib` directory as follows

   ```
   export LD_LIBRARY_PATH=LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
   ```

3. Change directory. For example:

   ```
   cd WEBGATE_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools
   ```

4. Run the following command to copy the file `apache_webgate.template` from the WebGate home directory to the WebGate instance location (renamed to `webgate.conf`) and update the `httpd.conf` file to add one line to include the name of `webgate.conf`.

   ```
   ./EditHttpConf -w WEB_ORACLE_INSTANCE/config/OHS/component_name -oh WEBGATE_
   ORACLE_HOME
   ```

5. Copy the files `ObAccessClient.xml`, `cwallet.sso`, and `password.xml`, which were generated when you created the external agent from the directory

   ```
   IAD_ASERVER_HOME/output/Webgate_External
   ```

   on IDMHOST1, to the directory:

   ```
   WEB_ORACLE_INSTANCE/config/OHS/component_name/webgate/config
   ```

6. Copy The files `aaa_key.pem` and `aaa_cert.pem`, which were generated when you created the agent from the directory

   ```
   IAD_ASERVER_HOME/output/Webgate_External
   ```

   on IDMHOST1 to the WebGate instance directory:

   ```
   WEB_ORACLE_INSTANCE/config/OHS/component_name/webgate/config/simple
   ```

7. Restart the Oracle HTTP Server

D.5 Validating the Installation

Test the installation by trying to access the protected resource:

```
http://external_ohs/sso.html
```

You are redirected to the OAM credential collector. Enter a valid user name and password. The test page is displayed.