

Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity Management

11g Release 1 (11.1.1)

E12035-04

July 2010

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

E12035-04

Copyright © 2004, 2010, Oracle and/or its affiliates. All rights reserved.

Primary Author: Ellen Desmond

Contributing Authors: Bharath K. Reddy, Michael Rhys

Contributors: Janga Aliminati, Rajesh Bhabu, Pradeep Bhat, Eileen He, Jean Jayet, Xiao Lin, Nicolas Philippe, Bert Rich, Vinay Shukla, Kamal Singh

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xvii
Audience	xvii
Documentation Accessibility	xvii
Related Documents	xviii
Conventions	xix
1 Enterprise Deployment Overview	
1.1 What is an Enterprise Deployment?	1-1
1.2 Terminology	1-2
1.3 Benefits of Oracle Recommendations	1-3
1.3.1 Built-in Security	1-3
1.3.2 High Availability	1-4
1.4 The Enterprise Deployment Reference Topologies	1-4
1.4.1 Topology 1 - Oracle Access Manager 11g	1-4
1.4.1.1 Understanding the Directory Tier	1-5
1.4.1.2 Understanding the Application Tier	1-6
1.4.1.3 Understanding the Web Tier	1-7
1.4.2 Topology 2 - Oracle Access Manager 10g and Oracle Identity Manager 11g	1-8
1.4.2.1 Understanding the Directory Tier	1-9
1.4.2.2 Understanding the Application Tier	1-10
1.4.2.3 Understanding the Web Tier	1-12
1.4.3 Topology 3 - Oracle Access Manager 11g and Oracle Identity Manager 11g	1-13
1.4.3.1 Understanding the Directory Tier	1-14
1.4.3.2 Understanding the Application Tier	1-15
1.4.3.3 Understanding the Web Tier	1-17
1.4.4 Topology 4 - Oracle Adaptive Access Manager 11g	1-17
1.4.4.1 Understanding the Directory Tier	1-18
1.4.4.2 Understanding the Application Tier	1-19
1.4.4.3 Understanding the Web Tier	1-20
1.4.5 Topology 5 - Oracle Identity Federation 11g	1-21
1.4.5.1 Understanding the Directory Tier	1-22
1.4.5.2 Understanding the Application Tier	1-23
1.4.5.3 Understanding the Web Tier	1-24
1.5 Using This Guide	1-25

2 Prerequisites for Enterprise Deployments

2.1	Hardware Resource Planning	2-1
2.2	Network Prerequisites.....	2-2
2.2.1	Load Balancers	2-2
2.2.2	Configuring Virtual Server Names and Ports on the Load Balancer	2-3
2.2.3	Administration Server Virtual IP Address	2-4
2.2.4	Managing Oracle Fusion Middleware Component Connections.....	2-5
2.2.5	Oracle Access Manager Communication Protocol and Terminology.....	2-5
2.2.5.1	Oracle Access Manager Protocols	2-5
2.2.5.2	Overview of User Request.....	2-5
2.2.6	Firewall and Port Configuration	2-5
2.3	WebLogic Domain Considerations	2-8
2.4	Shared Storage and Recommended Directory Structure	2-8
2.4.1	Directory Structure Terminology and Environment Variables	2-8
2.4.2	Recommended Locations for the Different Directories.....	2-9

3 Configuring the Database Repositories

3.1	Real Application Clusters	3-3
3.2	Configuring the Database for Oracle Fusion Middleware 11g Metadata.....	3-3
3.3	Executing the Repository Creation Utility	3-5
3.3.1	Procedure for Executing RCU.....	3-5
3.3.2	RCU Example	3-7

4 Installing the Software

4.1	Introduction	4-1
4.2	Using this Guide	4-1
4.3	Software Installation Summary	4-2
4.4	Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2	4-4
4.4.1	Prerequisites	4-4
4.4.1.1	Check Port 7777.....	4-4
4.4.1.2	Check oraInst.loc	4-4
4.4.2	Installation	4-4
4.4.3	Upgrading Oracle HTTP Server from 11.1.1.2 to 11.1.1.3	4-5
4.5	Installing Oracle Fusion Middleware	4-6
4.5.1	Installing Oracle Fusion Middleware Components.....	4-6
4.5.2	Installing Oracle Fusion Middleware Home	4-6
4.5.3	Installing Oracle WebLogic Server.....	4-7
4.5.4	Installing the Oracle Identity Management Platform and Directory Services Suite..	4-8
4.5.5	Installing the Oracle Identity and Access Management Suite	4-9
4.5.6	Installing the Oracle SOA Suite	4-11
4.6	Upgrading the Oracle Homes for Oracle Identity Management Suite and Oracle SOA from 11.1.1.2 to 11.1.1.3	4-12
4.6.1	Upgrading the Oracle Identity Management Platform and Directory Services Suite Oracle Home	4-12
4.6.2	Upgrading the Oracle SOA Suite Oracle Home.....	4-13
4.7	Patching the Software.....	4-13

4.7.1	Patch 9745107	4-13
4.7.2	Patch 9449855	4-14
4.7.3	Patch 9824531	4-17
4.7.4	Patch 9477292	4-19
4.7.5	Creating the wfullclient.jar File	4-22
4.7.6	Provisioning the Oracle Identity Manager Login Modules Under the WebLogic Server Library Directory 4-22	
4.7.7	Patch 9847606	4-23
4.8	Upgrading Existing Enterprise Deployment Topologies	4-23
4.9	Backing Up the Installation	4-23

5 Configuring the Web Tier

5.1	Configuring the Web Tier	5-1
5.2	Configuring the Oracle Web Tier	5-1
5.2.1	Validating the Installation	5-2
5.3	Configuring Oracle HTTP Server with the Load Balancer	5-3
5.4	Configuring Virtual Hosts	5-3
5.5	Validating the Installation	5-3

6 Creating the WebLogic Server Domain for Identity Management

6.1	Enabling ADMINVHN on IDMHOST1.....	6-1
6.2	Running the Configuration Wizard on IDMHOST1 to Create a Domain	6-2
6.3	Creating boot.properties for the Administration Server on IDMHOST1	6-5
6.4	Starting Node Manager on IDMHOST1	6-5
6.5	Updating the Node Manager Credentials.....	6-6
6.6	Disabling Host Name Verification for the Oracle WebLogic Administration Server	6-7
6.7	Stopping and Starting the WebLogic Administration Server	6-7
6.8	Validating the Administration Server.....	6-8
6.9	Configuring Oracle HTTP Server for the Administration Server.....	6-8
6.10	Registering Oracle HTTP Server With WebLogic Server.....	6-9
6.11	Setting the Front End URL for the Administration Console	6-9
6.12	Validating Access Through Oracle HTTP Server.....	6-10
6.13	Manually Failing Over the Administration Server	6-10
6.13.1	Failing over the Administration Server to IDMHOST2	6-10
6.13.2	Starting the Administration Server on IDMHOST2	6-11
6.13.3	Validating Access to IDMHOST2 Through Oracle HTTP Server.....	6-12
6.13.4	Failing the Administration Server Back to IDMHOST1.....	6-12
6.14	Backing Up the Installation	6-13

7 Extending the Domain with Oracle Internet Directory

7.1	Prerequisites for Configuring Oracle Identity Directory Instances.....	7-1
7.1.1	Synchronizing the Time on Oracle Internet Directory	7-1
7.2	Configuring the Oracle Internet Directory Instances	7-2
7.2.1	Configure the First Oracle Internet Directory Instance.....	7-2
7.2.2	Configuring an Additional Oracle Internet Directory Instance.....	7-4
7.3	Post Configuration Steps	7-7

7.3.1	Registering Oracle Internet Directory with the Oracle WebLogic Server Domain.....	7-7
7.4	Validating the Oracle Internet Directory Instances	7-8
7.5	Backing up the OID Configuration	7-9

8 Extending the Domain with Oracle Virtual Directory

8.1	Prerequisites for Configuring Oracle Virtual Directory Instances	8-1
8.1.1	Software, Network, and Directory Structure.....	8-1
8.2	Configuring the Oracle Virtual Directory Instances	8-1
8.2.1	Configuring the First Oracle Virtual Directory Instance	8-2
8.2.2	Configuring an Additional Oracle Virtual Directory	8-3
8.3	Post Configuration Steps	8-5
8.3.1	Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain	8-5
8.3.2	Creating Server Certificates for the Oracle Virtual Directory Instances.....	8-6
8.3.3	Configuring Adapters in Oracle Virtual Directory	8-7
8.4	Validating the Oracle Virtual Directory Instances	8-8
8.5	Backing Up the Oracle Virtual Directory Configuration	8-8

9 Extending the Domain with Oracle Directory Integration Platform and ODSM

9.1	Extending the Oracle WebLogic Domain with Oracle Directory Integration Platform and ODSM	9-1
9.2	Expanding the Oracle Directory Integration Platform and ODSM Cluster	9-4
9.2.1	Installing and Configuring Oracle Directory Integration Platform and ODSM on IDMHOST2	9-4
9.2.2	Post-Installation Steps.....	9-6
9.2.2.1	Copying the DIP Application from IDMHOST1 to IDMHOST2.....	9-7
9.2.2.2	Setting the Listen Address for the Managed Servers	9-7
9.2.2.3	Starting the Managed Server on IDMHOST2.....	9-7
9.3	Provisioning the Managed Servers on the Local Disk.....	9-8
9.4	Validating the Application Tier Configuration	9-9
9.4.1	Validating Oracle Directory Services Manager	9-9
9.4.2	Validating Oracle Directory Integration Platform.....	9-10
9.5	Creating the Oracle Internet Directory Adapter Using ODSM.....	9-11
9.6	Backing Up the Application Tier Configuration	9-12

10 Extending the Domain with Oracle Access Manager 10g

10.1	Introduction to Installing Oracle Access Manager.....	10-1
10.1.1	Using 10g Oracle Single Sign-On and Delegated Administration Services	10-2
10.1.2	Using Different LDAP Directory Stores	10-2
10.1.2.1	Using Oracle Virtual Directory as the Identity Store	10-2
10.2	Prerequisites	10-2
10.2.1	Making libgcc_s.so.1 and libstdc++.so.5 Available	10-3
10.2.2	Working Around the Installer Bug	10-3
10.3	Identity System Installation and Configuration.....	10-3
10.3.1	Installing Identity Servers on OAMHOST1 and OAMHOST2	10-3
10.3.1.1	Installing the First Identity Server on OAMHOST1	10-3
10.3.1.2	Installing the Second Identity Server on OAMHOST2	10-7

10.3.2	Installing Oracle HTTP Server on OAMADMINHOST	10-10
10.3.2.1	Installing Oracle HTTP Server	10-10
10.3.2.2	Validating the Installation of Oracle HTTP Server	10-12
10.3.3	Installing WebPass on OAMADMINHOST	10-13
10.3.3.1	Validating the WebPass Installation	10-16
10.3.4	Configuring Identity Servers Using WebPass	10-16
10.3.4.1	Configuring the First Identity Server	10-16
10.3.4.2	Configuring the Second Identity Server	10-20
10.4	Access System Installation and Configuration	10-22
10.4.1	Installing the Policy Manager on OAMADMINHOST	10-22
10.4.1.1	Configuring the Policy Manager	10-25
10.4.2	Installing the Access Server on OAMHOST1 and OAMHOST2	10-30
10.4.2.1	Creating an Access Server Instance	10-30
10.4.2.2	Starting the Access Server Installation	10-32
10.4.3	Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2	10-35
10.4.3.1	About the Oracle Access Manager Configuration Tool	10-35
10.4.3.2	Collecting the Information for the OAM Configuration Tool	10-35
10.4.3.3	Running the OAM Configuration Tool	10-36
10.4.3.4	Updating the Host Identifier	10-38
10.4.3.5	Updating the WebGate Profile	10-39
10.4.3.6	Assigning an Access Server to the WebGate	10-40
10.4.3.7	Installing the WebGate	10-40
10.5	Backing Up the Oracle Access Manager Configuration	10-44

11 Extending the Domain with Oracle Access Manager 11g

11.1	Introduction to Installing Oracle Access Manager	11-1
11.1.1	Using Different LDAP Directory Stores	11-2
11.1.2	Using Oracle Virtual Directory as the Identity Store	11-2
11.2	Prerequisites	11-2
11.3	Configuring Oracle Access Manager on IDMHOST1	11-2
11.3.1	Starting Oracle Access Manager Server on IDMHOST1	11-5
11.3.2	Propagating the Domain Changes to the Managed Server Domain Directory	11-5
11.3.3	Remove IDM Domain Agent	11-5
11.4	Configure Oracle Access Manager on IDMHOST2	11-6
11.4.1	Updating Node Manager Properties File on IDMHOST2	11-6
11.4.2	Starting Oracle Access Manager Server on IDMHOST2	11-6
11.5	Configuring Oracle Access Manager to work with the Oracle Web Tier	11-6
11.5.1	Prerequisites	11-7
11.5.2	Making Oracle Access Manager Server Aware of Load balancer	11-7
11.5.3	Configuring Oracle HTTP Servers to Display Login Page	11-7
11.5.4	Configuring Oracle HTTP Servers to Access Oracle Access Manager Console	11-7
11.5.5	Validating Accessibility	11-8
11.6	Changing Request Cache Type	11-8
11.7	Configuring Oracle Access Manager to use an External LDAP store	11-9
11.7.1	Creating Users and Groups in LDAP	11-9
11.7.2	Backing up Existing Configuration	11-10
11.7.3	Creating User Identity Store	11-10

11.7.4	Setting LDAP to Primary Authentication Store	11-10
11.7.5	Validating the Configuration	11-11
11.8	Creating Policy Groups	11-11
11.8.1	Creating Oracle Access Manager Policy Group	11-11
11.8.2	Creating Oracle Adaptive Access ManagerPolicy Group	11-12
11.9	Validating Oracle Access Manager	11-12
11.9.1	Creating a Test Resource	11-12
11.9.2	Creating a Resource	11-12
11.9.3	Assigning Resource to Policy Group	11-13
11.9.4	Adding Resource to Protected Resources	11-13
11.9.5	Validating Oracle Access Manager	11-13

12 Extending the Domain with Oracle Adaptive Access Manager

12.1	Prerequisites	12-1
12.1.1	Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP. 12-2	
12.2	Configuring Oracle Adaptive Access Manager on IDMHOST1	12-3
12.2.1	Extending Domain for Oracle Adaptive Access Manager	12-4
12.2.2	Starting Admin Server on IDMHOST1	12-8
12.2.3	Creating Oracle Adaptive Access Manager Administration User in WebLogic Console. 12-8	
12.2.4	Configuring Oracle Adaptive Access Manager on OAAMHOST1	12-9
12.3	Start OAAMHOST1	12-9
12.3.1	Creating Node Manager Properties File on OAAMHOST1	12-9
12.3.2	Starting Oracle Adaptive Access Manager on OAAMHOST1	12-9
12.3.3	Validating OAAMHOST1	12-9
12.4	Configuring Oracle Adaptive Access Manager on OAAMHOST2	12-10
12.4.1	Deploying Domain on OAAMHOST2	12-10
12.4.2	Starting OAAMHOST2	12-10
12.4.2.1	Creating Node Manager Properties File on OAAMHOST2	12-10
12.4.2.2	Starting Oracle Adaptive Access Manager on OAAMHOST2	12-10
12.4.3	Validating OAAMHOST2	12-10
12.5	Configuring Oracle Adaptive Access Manager to Work with the Oracle HTTP Server	12-11
12.5.1	Updating Oracle HTTP Server configuration	12-11
12.5.2	Restarting Oracle HTTP Server	12-12
12.5.3	Changing Host Assertion in WebLogic	12-12
12.5.4	Validating Oracle Adaptive Access Manager	12-13
12.6	Loading Oracle Adaptive Access Manager Seed Data	12-13
12.6.1	Loading Default Policies into OAAM Repository	12-13
12.6.2	Loading Knowledge Based Authentication Questions into Oracle Adaptive Access Manager Repository 12-13	
12.6.3	Loading Location data into Oracle Adaptive Access Manager Repository	12-14

13 Extending the Domain with Oracle Identity Manager

13.1	Prerequisites	13-2
------	---------------------	------

13.2	Extending the Domain to Configure Oracle Identity Manager and Oracle SOA Suite on IDMHOST1	13-2
13.3	Configuring Oracle Identity Manager on IDMHOST1	13-6
13.3.1	Prerequisites for Configuring Oracle Identity Manager	13-6
13.3.1.1	Configuring Oracle Internet Directory using the LDAP Configuration Pre-setup Script	13-6
13.3.1.2	Creating Adapters in Oracle Virtual Directory	13-8
13.3.2	Running the Oracle Identity Management Configuration Wizard	13-11
13.4	Propagating the Oracle Identity Manager and SOA Managed Servers to OIMHOST1 and OIMHOST2	13-13
13.5	Post-Installation Steps on OIMHOST1 and OIMHOST2	13-13
13.5.1	Updating the Coherence Configuration for the SOA Managed Server.....	13-13
13.5.2	Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1.....	13-15
13.5.3	Validating Oracle Identity Manager Instance on OIMHOST1.....	13-15
13.6	Post Installation Steps on OIMHOST2.....	13-15
13.6.1	Starting Node Manager on OIMHOST2.....	13-15
13.6.2	Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2.....	13-16
13.6.3	Validating Oracle Identity Manager Instance on OIMHOST2.....	13-16
13.7	Configuring Oracle Internet Directory using the LDAP Configuration Post setup Script	13-16
13.8	Configuring Oracle Identity Manager to Work with the Oracle Web Tier	13-17
13.8.1	Prerequisites	13-17
13.8.2	Configuring Oracle HTTP Servers to front end the OIM & SOA Managed Servers.	13-17
13.8.3	Validating Oracle Identity Manager Instance from the WebTier	13-18
13.9	Configuring a Shared JMS Persistence Store	13-19
13.10	Configuring a Default Persistence Store for Transaction Recovery	13-19
13.11	Adding the CSF Entries for Oracle Identity Management and WSM.....	13-20

14 Extending the Domain with Authorization Policy Manager and Identity Navigator

14.1	Extending the Domain with Oracle Authorization Policy Manager.....	14-1
14.1.1	Base Authorization Policy Manager Platform.....	14-2
14.1.2	Prerequisites	14-2
14.1.3	Configuring Authorization Policy Manager on IDMHOST1.....	14-2
14.1.4	Stopping and Starting the Admin Server IDMHOST1.....	14-3
14.1.5	Authorization Policy Manager on IDMHOST2.....	14-3
14.1.6	Configure Oracle HTTP Servers to Access Authorization Policy Manager Console	14-4
14.1.6.1	Validating the Implementation	14-5
14.1.7	Configuring Authorization Policy Manager to Use an External LDAP Store	14-5
14.2	Extending the Domain with Oracle Identity Navigator.....	14-5
14.2.1	Prerequisites	14-5
14.2.2	Configure Oracle Identity Navigator on IDMHOST1	14-5
14.2.3	Stopping and Starting the Administration Server IDMHOST1.....	14-6
14.2.4	Provisioning Oracle Identity Navigator on IDMHOST1	14-6
14.2.5	Configuring Oracle HTTP Servers to Access Oracle Identity Navigator Console..	14-6

14.2.6	Validating Oracle Identity Navigator	14-7
--------	--	------

15 Extending the Domain with Oracle Identity Federation

15.1	Prerequisites	15-1
15.2	Configuring Oracle Identity Federation on OIFHOST1	15-2
15.3	Configuring Oracle Identity Federation on OIFHOST2.....	15-6
15.4	Post-Installation Steps for Oracle Identity Federation	15-8
15.4.1	Copying the Oracle Identity Federation Configuration Directory from OIFHOST1 to OIFHOST2	15-8
15.4.2	Set the Listen Address for the Managed Servers	15-9
15.4.3	Starting the Managed Server on OIFHOST2	15-9
15.5	Provisioning the Managed Servers on the Local Disk.....	15-9
15.6	Enabling Oracle Identity Federation Integration with LDAP Servers	15-11
15.7	Configuring Oracle Identity Federation to work with the Oracle Web Tier.....	15-11
15.7.1	Prerequisites	15-11
15.7.2	Making OIF aware of the Load Balancer.....	15-12
15.7.3	Configuring Oracle HTTP Servers To Front End the OIF Managed Servers.....	15-12
15.8	Validating.....	15-12

16 Setting Up Node Manager

16.1	About Setting Up Node Manager.....	16-1
16.2	Changing the Location of the Node Manager Log	16-2
16.3	Enabling Host Name Verification Certificates for Node Manager.....	16-3
16.3.1	Generating Self-Signed Certificates Using the utils.CertGen Utility	16-3
16.3.2	Creating an Identity Keystore Using the utils.ImportPrivateKey Utility.....	16-4
16.3.3	Creating a Trust Keystore Using the Keytool Utility	16-5
16.3.4	Configuring Node Manager to Use the Custom Keystores.....	16-5
16.3.5	Configuring Managed WLS Servers to Use the Custom Keystores	16-6
16.3.6	Changing the Host Name Verification Setting for the Managed Servers	16-7
16.4	Starting Node Manager.....	16-8

17 Integrating Components

17.1	Migrating Policy and Credential Stores.....	17-1
17.1.1	JPS Root Creation.....	17-1
17.1.2	Reassociating the Policy and Credential Store	17-2
17.2	Installing and Configuring WebGate.....	17-3
17.2.1	Prerequisites	17-3
17.2.1.1	Making Special gcc Libraries Available	17-3
17.2.2	Creating WebGate Agents.....	17-3
17.2.2.1	Using the Remote Registration Utility	17-3
17.2.2.2	Using Oracle Access Manager Administration Console.....	17-5
17.2.2.3	Update Newly-Created Agent	17-6
17.2.3	Installing Oracle WebGate on WEBHOST1 and WEBHOST2	17-6
17.2.3.1	Oracle WebGate 10g.....	17-6
17.2.4	Validating WebGate	17-9
17.3	Integrating Administration Consoles with Single Sign-on 11g.....	17-9

17.3.1	Prerequisites	17-9
17.3.2	Creating Oracle Virtual Directory Authenticator	17-9
17.3.3	Creating Oracle Access Manager Identity Asserter.....	17-11
17.4	Integrating Oracle Access Manager 10g and Oracle Identity Manager	17-11
17.4.1	Prerequisites	17-11
17.4.1.1	Update the LDAP Schema Definitions	17-12
17.4.1.2	Patching the Access Server.....	17-12
17.4.2	Creating Policies in Oracle Access Manager 10g.....	17-12
17.4.3	Enabling Oracle Access Manager 10g and Oracle Identity Manager Integration .	17-14
17.4.4	Configuring Oracle Access Manager 10g/Oracle Identity Manager Authenticator.....	17-15
17.4.5	Configuring Auto-Login for Oracle Identity Manager	17-15
17.5	Integrating Oracle Identity Manager and Oracle Access Manager 11g.....	17-17
17.5.1	Prerequisites	17-17
17.5.2	Updating Single Sign-on Provider Configuration	17-17
17.5.3	Configure Oracle Access Manager for Oracle Identity Manager Integration.....	17-18
17.5.4	Integrating Oracle Access Manager with Oracle Identity Manager using the OIM Configuration Tool	17-19
17.5.4.1	Prerequisites	17-19
17.5.4.2	Using OIM Configuration Tool	17-19
17.5.5	Seed the xelsysadm User in Oracle Internet Directory	17-22
17.5.6	Updating Oracle Identity Manager Configuration.....	17-22
17.6	Integrating Oracle Adaptive Access Manager with Oracle Access Manager	17-25
17.6.1	Prerequisites	17-26
17.6.2	Configuring OAM Encryption Keys in CSF	17-26
17.6.3	Configuring OAM Policy Authentication Scheme	17-26
17.6.4	Setting OAAM properties for OAM	17-27
17.6.5	Validating Oracle Adaptive Access Manager/Oracle Identity Manager Integration.....	17-27
17.6.5.1	Creating a Resource.....	17-28
17.6.5.2	Assigning Resource to Policy Group.....	17-28
17.6.5.3	Adding Resource to Protected Resources	17-28
17.6.5.4	Validating Oracle Access Manager	17-29
17.7	Integrating Oracle Adaptive Access Manager with Oracle Identity Manager	17-29
17.7.1	Prerequisites	17-29
17.7.2	Configuring OIM Encryption Keys in CSF	17-29
17.7.3	Setting OAAM properties for OIM	17-30
17.7.4	Setting OIM properties for OAAM	17-31
17.7.5	Restarting Oracle Adaptive Access Manager and Oracle Identity Manager	17-31
17.7.6	Restarting Managed Servers	17-31
17.7.7	Validating OIM/OAAM Integration	17-31
17.8	Integrating Oracle Identity Federation with Oracle Access Manager.....	17-32
17.8.1	Configure Oracle Identity Federation Server	17-32
17.8.1.1	Generating and Configuring Identity Provider and Service Provider Modules	17-32
17.8.1.2	Configuring the Data Stores.....	17-32
17.8.1.3	Configuring the Authentication Engines	17-32

17.8.1.4	Configuring the Oracle Identity Federation Server in Service Provider Mode.....	
	17-33	
17.8.2	Configuring Oracle Access Manager Server.....	17-33
17.9	Auditing Identity Management.....	17-34

18 Managing Enterprise Deployments

18.1	Starting and Stopping Oracle Identity Management Components.....	18-1
18.1.1	Oracle Virtual Directory.....	18-1
18.1.2	Oracle Internet Directory.....	18-2
18.1.3	Oracle HTTP Server.....	18-2
18.1.4	Node Manager.....	18-2
18.1.5	WebLogic Administration Server.....	18-3
18.1.6	Oracle Identity Manager.....	18-3
18.1.7	Oracle Access Manager Managed Servers.....	18-4
18.1.8	Oracle Adaptive Access Manager Managed Servers.....	18-5
18.2	Monitoring Enterprise Deployments.....	18-5
18.2.1	Monitoring Oracle Internet Directory.....	18-5
18.2.1.1	Oracle Internet Directory Component Names Assigned by Oracle Identity Management Installer	18-6
18.2.2	Monitoring Oracle Virtual Directory.....	18-6
18.2.3	Monitoring Oracle Directory Integration Platform.....	18-7
18.2.4	Monitoring Oracle Access Manager.....	18-8
18.3	Scaling Enterprise Deployments.....	18-8
18.3.1	Scaling Up the Topology.....	18-8
18.3.1.1	Scaling Up the Directory Tier.....	18-8
18.3.1.1.1	Scaling Up Oracle Internet Directory.....	18-8
18.3.1.1.2	Scaling Up Oracle Virtual Directory.....	18-9
18.3.1.2	Scaling Up the Application Tier.....	18-9
18.3.1.2.1	Scaling Up Oracle Directory Integration Platform and Oracle Directory Services Manager	18-10
18.3.1.2.2	Scaling Up Oracle Access Manager 10g.....	18-10
18.3.1.2.3	Scaling Up Oracle Access Manager 11g.....	18-10
18.3.1.2.4	Scaling Up Oracle Adaptive Access Manager.....	18-12
18.3.1.3	Scaling Up Oracle Identity Manager (Adding Managed Servers to Existing Nodes)	18-13
18.3.1.4	Scaling Up the Web Tier.....	18-17
18.3.2	Scaling Out the Topology.....	18-17
18.3.2.1	Scaling Out the Directory Tier.....	18-17
18.3.2.1.1	Scaling Out Oracle Internet Directory.....	18-18
18.3.2.1.2	Scaling Out Oracle Virtual Directory.....	18-18
18.3.2.2	Scaling Out the Application Tier.....	18-18
18.3.2.2.1	Scaling Out Oracle Directory Integration Platform and Oracle Directory Services Manager	18-18
18.3.2.2.2	Scaling Out Oracle Access Manager 10g.....	18-19
18.3.2.2.3	Scaling Out Oracle Access Manager 11g.....	18-19
18.3.2.2.4	Scaling Out Oracle Adaptive Access Manager.....	18-21
18.3.2.3	Scaling Out Oracle Identity Manager (Adding Managed Servers to New Nodes)	18-23

18.3.2.4	Scaling Out the Web Tier.....	18-29
18.4	Performing Backups and Recoveries	18-29
18.5	Patching Enterprise Deployments.....	18-31
18.5.1	Patching an Oracle Fusion Middleware Source File.....	18-31
18.5.2	Patching Identity Management Components.....	18-31
18.6	Troubleshooting	18-32
18.6.1	Troubleshooting Oracle Internet Directory.....	18-32
18.6.2	Troubleshooting Oracle Virtual Directory	18-33
18.6.3	Troubleshooting Oracle Directory Integration Platform	18-33
18.6.4	Troubleshooting Oracle Directory Services Manager	18-34
18.6.5	Troubleshooting Oracle Access Manager.....	18-38
18.6.5.1	User is Redirected to the Login Screen After Activating Some Administration Console Changes 18-38	
18.6.5.2	User is Redirected to the Administration Console's Home Page After Activating Some Changes 18-39	
18.6.5.3	Oracle Access Manager Configuration Tool Does Not Remove Invalid URLs.....	18-39
18.7	Other Recommendations	18-39
18.7.1	Preventing Timeouts for SQL*Net Connections	18-40

19 Configuring Single Sign-on for Administration Consoles

19.1	Prerequisites	19-1
19.1.1	Creating WebLogic Administrative Users in an LDAP Directory	19-1
19.1.1.1	Provisioning Admin Users and Groups in an LDAP Directory	19-2
19.1.1.2	Assigning the Admin Role to the Admin Group.....	19-3
19.1.1.3	Updating the boot.properties File on IDMHOST1 and IDMHOST2	19-3
19.2	Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 10g. 19-5	
19.2.1	Prerequisites for Configuring Single Sign-On.....	19-5
19.2.1.1	Enable the Policy Protecting the Policy Manager	19-5
19.2.2	Updating the Form Authentication for Delegated Administration	19-5
19.2.3	Validating the Policy Domain and AccessGate Configurations.....	19-6
19.2.3.1	Validating the Policy Domain Configuration.....	19-6
19.2.3.2	Validating the AccessGate Configuration.....	19-7
19.2.4	Setting Up the WebLogic Authenticators.....	19-7
19.2.4.1	Setting Up the Oracle Internet Directory Authenticator.....	19-7
19.2.4.2	Setting Up the Oracle Access Manager Identity Asserter	19-8
19.2.4.3	Reordering Oracle Access Manager Identity Asserter, Oracle Internet Directory Authenticator, and Default Authenticator 19-9	
19.2.4.4	Stopping and Starting the WebLogic Administration Servers and Managed Servers 19-9	
19.2.5	Validating the Oracle Access Manager Single Sign-On Setup	19-10
19.3	Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 11g. 19-10	

Index

List of Figures

1-1	Oracle Access Manager 11g.....	1-5
1-2	Oracle Access Manager 10g and Oracle Identity Manager 11g	1-9
1-3	Oracle Access Manager 11g and Oracle Identity Manager 11g	1-14
1-4	Oracle Adaptive Access Manager 11g	1-18
1-5	Oracle Identity Federation 11g.....	1-22
2-1	Directory Structure for Identity Management.....	2-12
6-1	Select Domain Source Screen	6-3
17-1	Audit Event Flow	17-35

List of Tables

1-1	Oracle Fusion Middleware Architecture Terminology	1-2
2-1	Typical Hardware Requirements	2-1
2-2	Ports Used in the Oracle Identity Management Enterprise Deployment topologies	2-6
2-3	Recommended Directory Structure.....	2-10
2-4	Directory Structure Elements.....	2-12
3-1	Mapping between Topologies, Databases and Schemas.....	3-1
3-2	Minimum Initialization Parameters for Oracle RAC Database	3-4
4-1	Software to be Installed for Different Topologies	4-2
4-2	Software Versions Used	4-3
4-3	Summary of Homes	4-6
10-1	Basic Parameters for the OAM Configuration Tool.....	10-36
10-2	OAM Configuration Tool Optional Parameters for CREATE Mode	10-37
16-1	Hosts in Each Topology	16-1
18-1	Static Artifacts to Back Up in the Identity Management Enterprise Deployment	18-29
18-2	Runtime Artifacts to Back Up in the Identity Management Enterprise Deployments	18-31

Preface

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

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

Related Documents

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

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

Also see the Oracle Access Manager 10g documentation in the Oracle Identity Management 10g (10.1.4) library at

<http://www.oracle.com/technology/documentation>.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

Enterprise Deployment Overview

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

This chapter includes the following topics:

- [Section 1.1, "What is an Enterprise Deployment?"](#)
- [Section 1.2, "Terminology"](#)
- [Section 1.3, "Benefits of Oracle Recommendations"](#)
- [Section 1.4, "The Enterprise Deployment Reference Topologies"](#)
- [Section 1.5, "Using This Guide"](#)

1.1 What is an Enterprise Deployment?

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

An Oracle Fusion Middleware enterprise deployment:

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

For more information on high availability practices, visit:

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

1.2 Terminology

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

Table 1–1 Oracle Fusion Middleware Architecture Terminology

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

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

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

1.3 Benefits of Oracle Recommendations

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

1.3.1 Built-in Security

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

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

1.3.2 High Availability

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

1.4 The Enterprise Deployment Reference Topologies

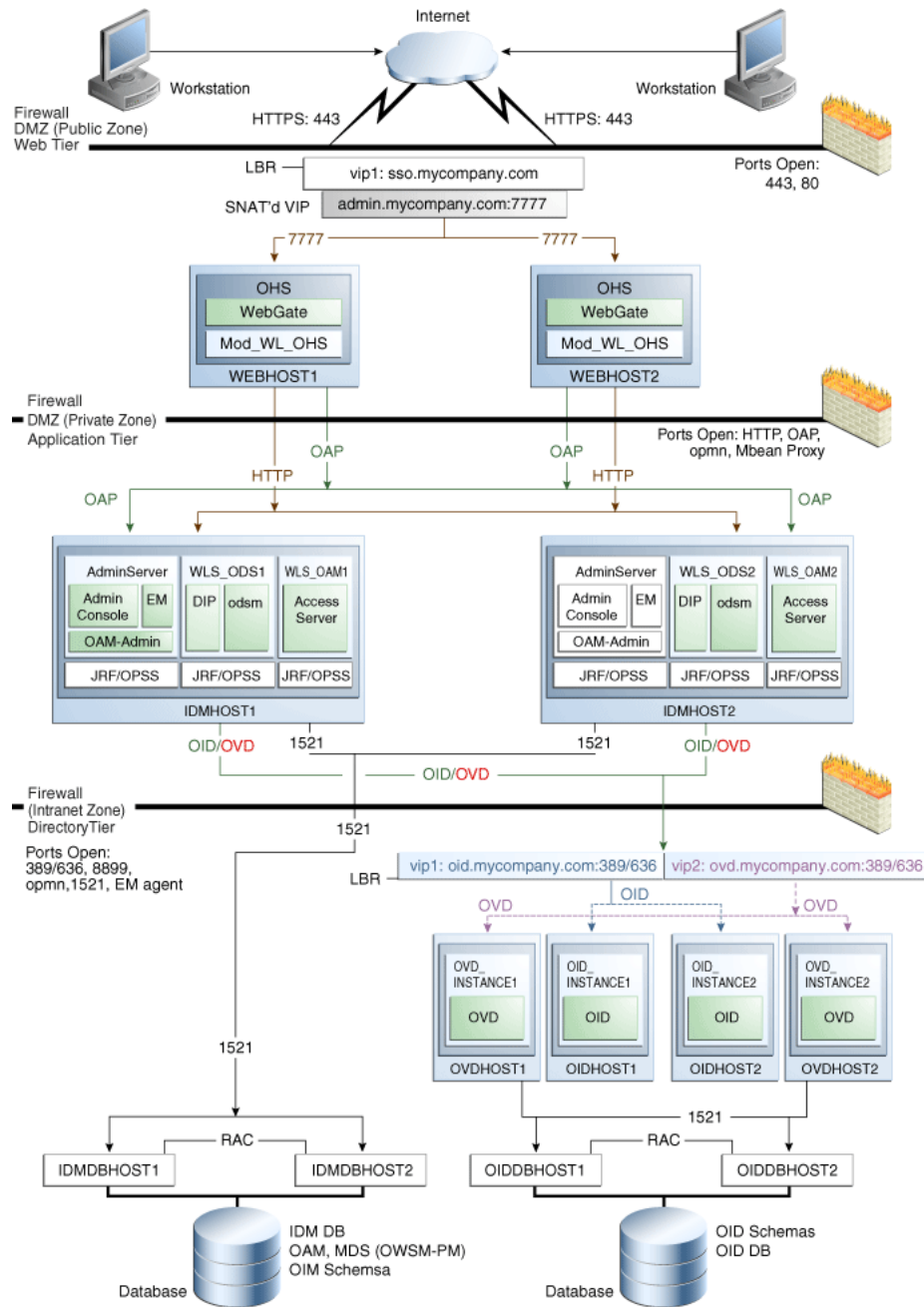
Oracle Identity Management consists of a number of products, which can be used either individually or collectively. The Enterprise Deployment Guide for Identity Management allows you to build five different enterprise topologies. This section describes them.

- [Section 1.4.1, "Topology 1 - Oracle Access Manager 11g"](#)
- [Section 1.4.2, "Topology 2 - Oracle Access Manager 10g and Oracle Identity Manager 11g"](#)
- [Section 1.4.3, "Topology 3 - Oracle Access Manager 11g and Oracle Identity Manager 11g"](#)
- [Section 1.4.4, "Topology 4 - Oracle Adaptive Access Manager 11g"](#)
- [Section 1.4.5, "Topology 5 - Oracle Identity Federation 11g"](#)

1.4.1 Topology 1 - Oracle Access Manager 11g

[Figure 1–1](#) is a diagram of the Oracle Access Manager 11g topology.

Figure 1–1 Oracle Access Manager 11g



1.4.1.1 Understanding the Directory Tier

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

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

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

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

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

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

1.4.1.2 Understanding the Application Tier

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

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

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

In the application tier:

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

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

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

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server, Oracle Enterprise Manager and Oracle Access Manager console are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- The WLS_OAM1 Managed Server on IDMHOST1 and WLS_OAM2 Managed Server on IDMHOST2 are in a cluster and the Access Manager applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.

High Availability Provisions

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

Security Provisions

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

1.4.1.3 Understanding the Web Tier

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

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

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

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the `mod_wl_ohs` plug-in module installed. The `mod_wl_ohs` plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.

- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on `IDMHOST1` and `IDMHOST2`, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

Architecture Notes

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

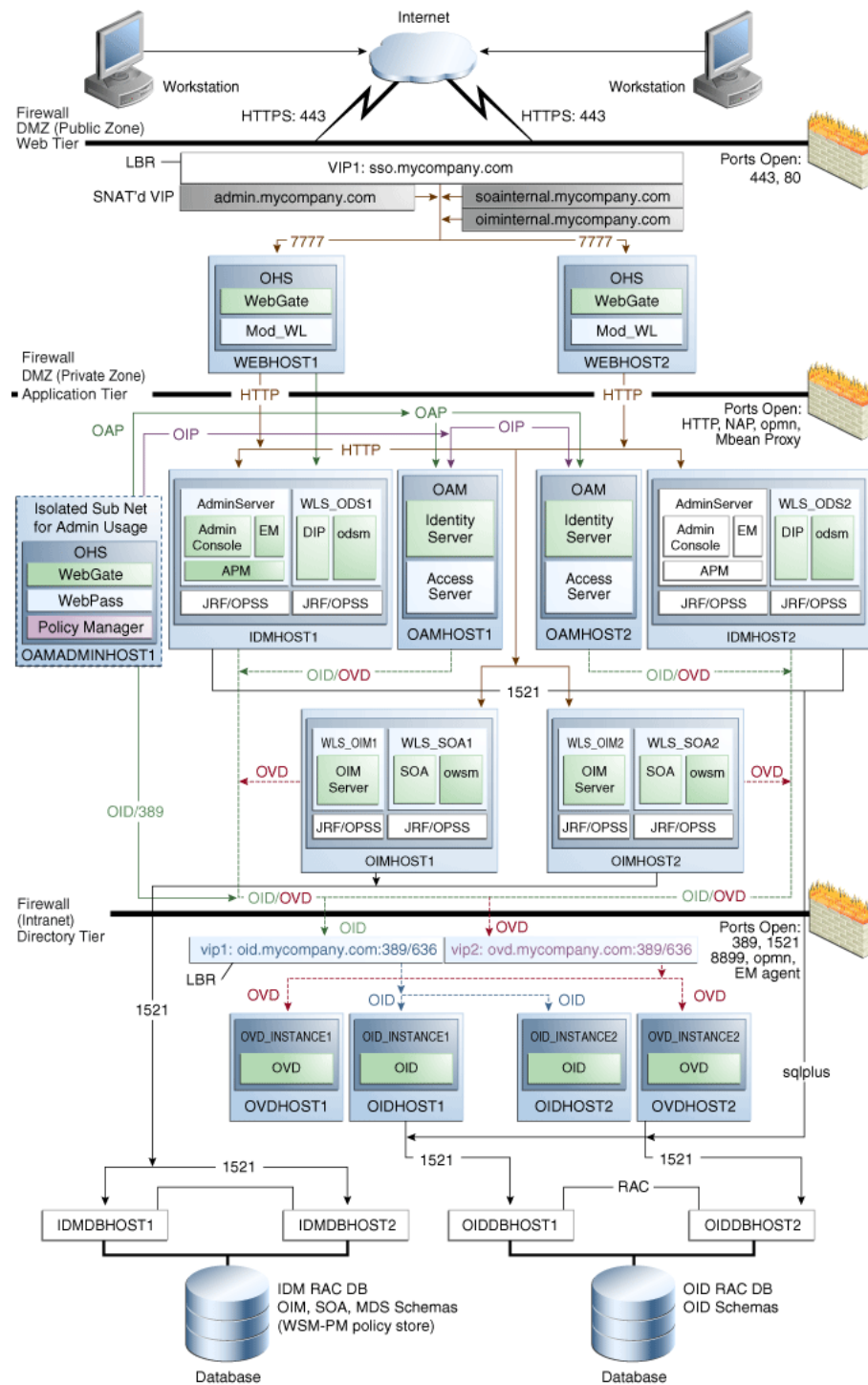
Security Provisions

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

1.4.2 Topology 2 - Oracle Access Manager 10g and Oracle Identity Manager 11g

[Figure 1–2](#) is a diagram of the Oracle Access Manager 10g and Oracle Identity Manager 11g topology.

Figure 1-2 Oracle Access Manager 10g and Oracle Identity Manager 11g



1.4.2.1 Understanding the Directory Tier

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

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

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

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

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

1.4.2.2 Understanding the Application Tier

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

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

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

In the application tier:

- `IDMHOST1` and `IDMHOST2` have the WebLogic Server with the Administration Console, Oracle Enterprise Manager Fusion Middleware Control, Oracle Directory Integration Platform, and Oracle Directory Services Manager installed. `IDMHOST1` and `IDMHOST2` run both the WebLogic Server Administration Servers and Managed Servers. Note that the administration server is configured to be active-passive, that is, although it is installed on both nodes, only one instance is active at any time. If the active instance goes down, then the passive instance starts up and becomes the active instance.
- On the firewall protecting the application tier, the HTTP ports, OIP port, and OAP port are open. The OIP (Oracle Identity Protocol) port is for the WebPass module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as querying user groups. The OAP (Oracle Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.

- OAMHOST1 and OAMHOST2 have Oracle Access Manager (with the Identity Server and Access Server components) installed. Oracle Access Manager is the single sign-on component for Oracle Fusion Middleware. It communicates with Oracle Internet Directory in the directory tier to verify user information.
- OIMHOST1 and OIMHOST2 have Oracle Identity Manager and Oracle SOA installed. Oracle Identity Manager is used for provisioning. Oracle SOA is used to provide the workflow functionality.

OAMADMINHOST is on an isolated subnet (for Oracle Access Manager administration), and it has Oracle HTTP Server, WebGate, WebPass, and Policy Manager installed.

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server, Oracle Enterprise Manager and Oracle Access Manager console are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.
- The WLS_OIM1 Managed Server on OIMHOST1 and WLS_OIM2 Managed Server on OIMHOST2 are in a cluster and the Oracle Identity Manager applications are targeted to the cluster.
- The WLS_SOA1 Managed Server on OIMHOST1 and WLS_SOA2 Managed Server on OIMHOST2 are in a cluster and the Oracle SOA applications are targeted to the cluster.

High Availability Provisions

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

Security Provisions

- Oracle WebLogic Server Console, Oracle Enterprise Manager Fusion Middleware Control console and Oracle Access Manager console are only

accessible through `admin.mycompany.com`, which is only available inside the firewall.

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

1.4.2.3 Understanding the Web Tier

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

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

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

In the web tier:

- `WEBHOST1` and `WEBHOST2` have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the `mod_wl_ohs` plug-in module installed. The `mod_wl_ohs` plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on `IDMHOST1` and `IDMHOST2`, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

Architecture Notes

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

Security Provisions

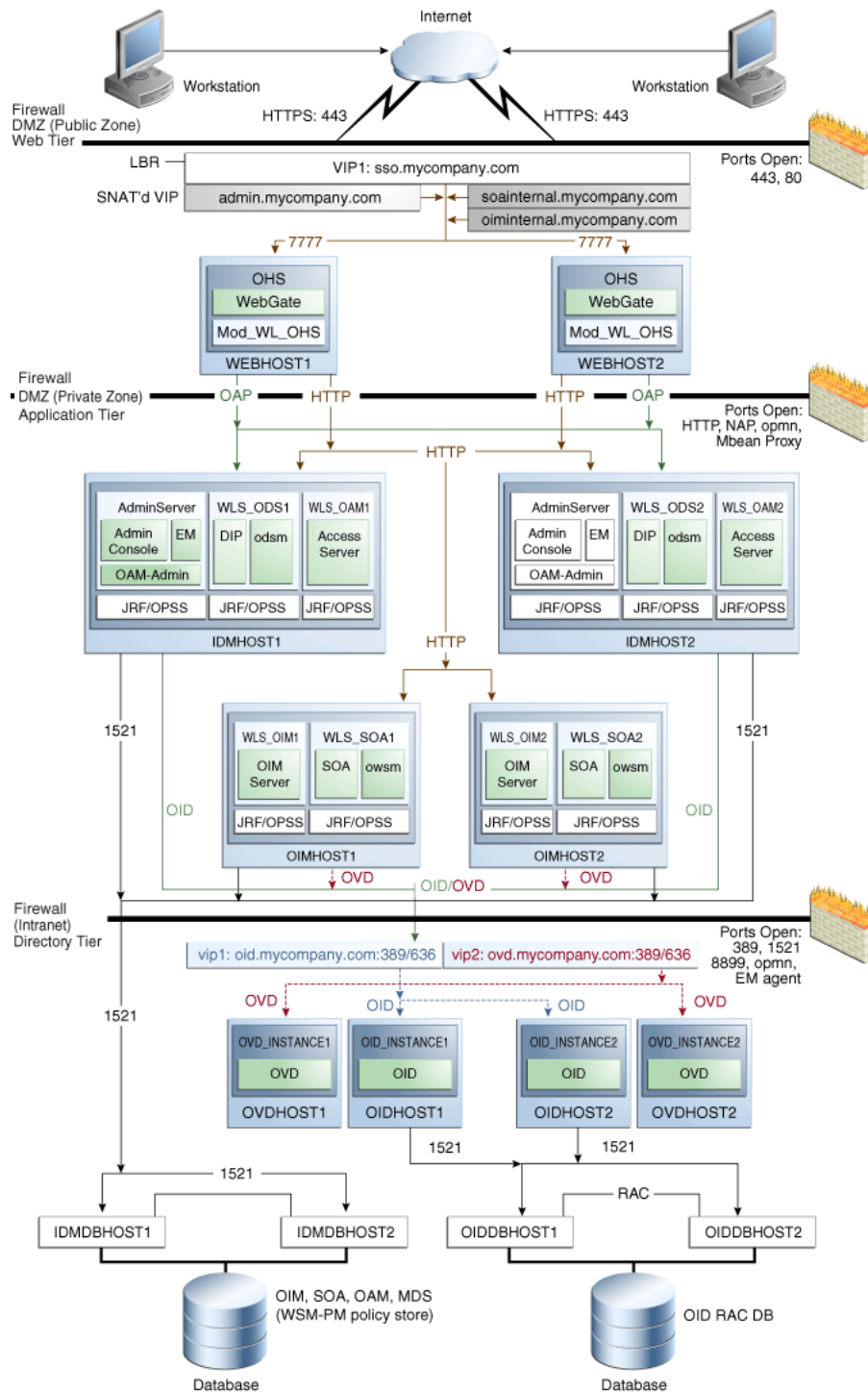
- The Oracle HTTP Servers process requests, received using the URL's `sso.mycompany.com` and `admin.mycompany.com`. The name `admin.mycompany.com` is only resolvable inside the firewall. This prevents access to sensitive resources such as the Oracle WebLogic Server console and Oracle Enterprise Manager Fusion Middleware Control console from the public domain.
- WebPass is installed on `OAMADMINHOST` along with the Policy Manager. The Policy Manager and the WebPass are used to configure the Access Servers and the Identity Servers on `OAMHOST1` and `OAMHOST2`.
- WebGate is installed on `OAMADMINHOST` to protect the Policy Manager, and configured on `WEBHOST1` and `WEBHOST2` to protect inbound access.

- Oracle Access Manager Identity Assertion Provider for WebLogic Server 11gR1 is installed on IDMHOST1 and IDMHOST2.

1.4.3 Topology 3 - Oracle Access Manager 11g and Oracle Identity Manager 11g

[Figure 1-1](#) is a diagram of the Oracle Access Manager 11g and Oracle Identity Manager 11g topology.

Figure 1-3 Oracle Access Manager 11g and Oracle Identity Manager 11g



1.4.3.1 Understanding the Directory Tier

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

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

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

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

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

1.4.3.2 Understanding the Application Tier

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

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

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

In the application tier:

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

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

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

in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.

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

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Access Manager console are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- The WLS_OAM1 Managed Server on IDMHOST1 and WLS_OAM2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Access Manager applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.
- The WLS_OIM1 Managed Server on OIMHOST1 and WLS_OIM2 Managed Server on OIMHOST2 are in a cluster and the Oracle Identity Manager applications are targeted to the cluster.
- The WLS_SOA1 Managed Server on OIMHOST1 and WLS_SOA2 Managed Server on OIMHOST2 are in a cluster and the Oracle SOA applications are targeted to the cluster.

High Availability Provisions

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

Security Provisions

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

1.4.3.3 Understanding the Web Tier

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

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

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

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the `mod_wl_ohs` plug-in module installed. The `mod_wl_ohs` plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on IDMHOST1 and IDMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

Architecture Notes

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

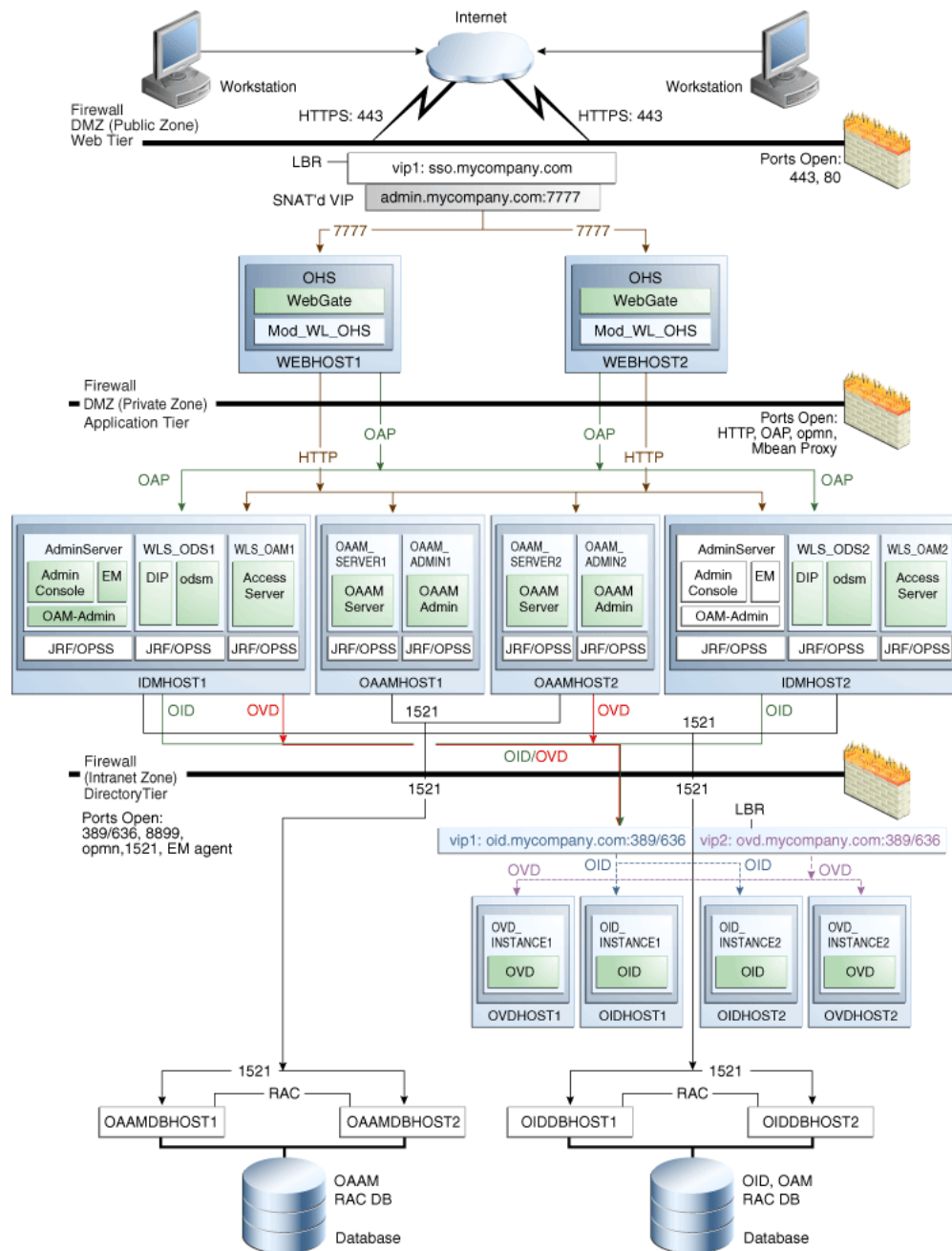
Security Provisions

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

1.4.4 Topology 4 - Oracle Adaptive Access Manager 11g

Figure 1–4 is a diagram of the Oracle Adaptive Access Manager 11g topology.

Figure 1–4 Oracle Adaptive Access Manager 11g



1.4.4.1 Understanding the Directory Tier

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

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

- Oracle Internet Directory relies on RDBMS as its backend.

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

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

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

1.4.4.2 Understanding the Application Tier

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

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

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

In the application tier:

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

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

- On the firewall protecting the application tier, the HTTP ports, OIP port, and OAP port are open. The OIP (Oracle Identity Protocol) port is for the WebPass module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as querying user groups. The OAP (Oracle Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.
- `OAAMHOST1` and `OAAMHOST2` have the WebLogic Server with the Oracle Adaptive Access Manager Server and Console installed.

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server, Oracle Enterprise Manager and Oracle Access Manager console are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- The WLS_OAM1 Managed Server on IDMHOST1 and WLS_OAM2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Access Manager applications are targeted to the cluster.
- The WLS_OAAM1 Managed Server on OAAMHOST1 and WLS_OAAM2 Managed Server on OAAMHOST2 are in a cluster and the Oracle Adaptive Access server applications are targeted to the cluster.
- The WLS_OAAM_ADMIN1 Managed Server on OAAMHOST1 and WLS_OAAM_ADMIN2 Managed Server on OAAMHOST2 are in a cluster and the Oracle Adaptive Access Administration console applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.

High Availability Provisions

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

Security Provisions

Oracle WebLogic Console, Oracle Fusion Middleware Console and Oracle Access Manager Console and Oracle Adaptive Access Manager console are only accessible via admin.mycompany.com, which is only available inside the firewall.

1.4.4.3 Understanding the Web Tier

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

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

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

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the mod_wl_ohs plug-in module installed. The mod_wl_ohs plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on IDMHOST1 and IDMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

Architecture Notes

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

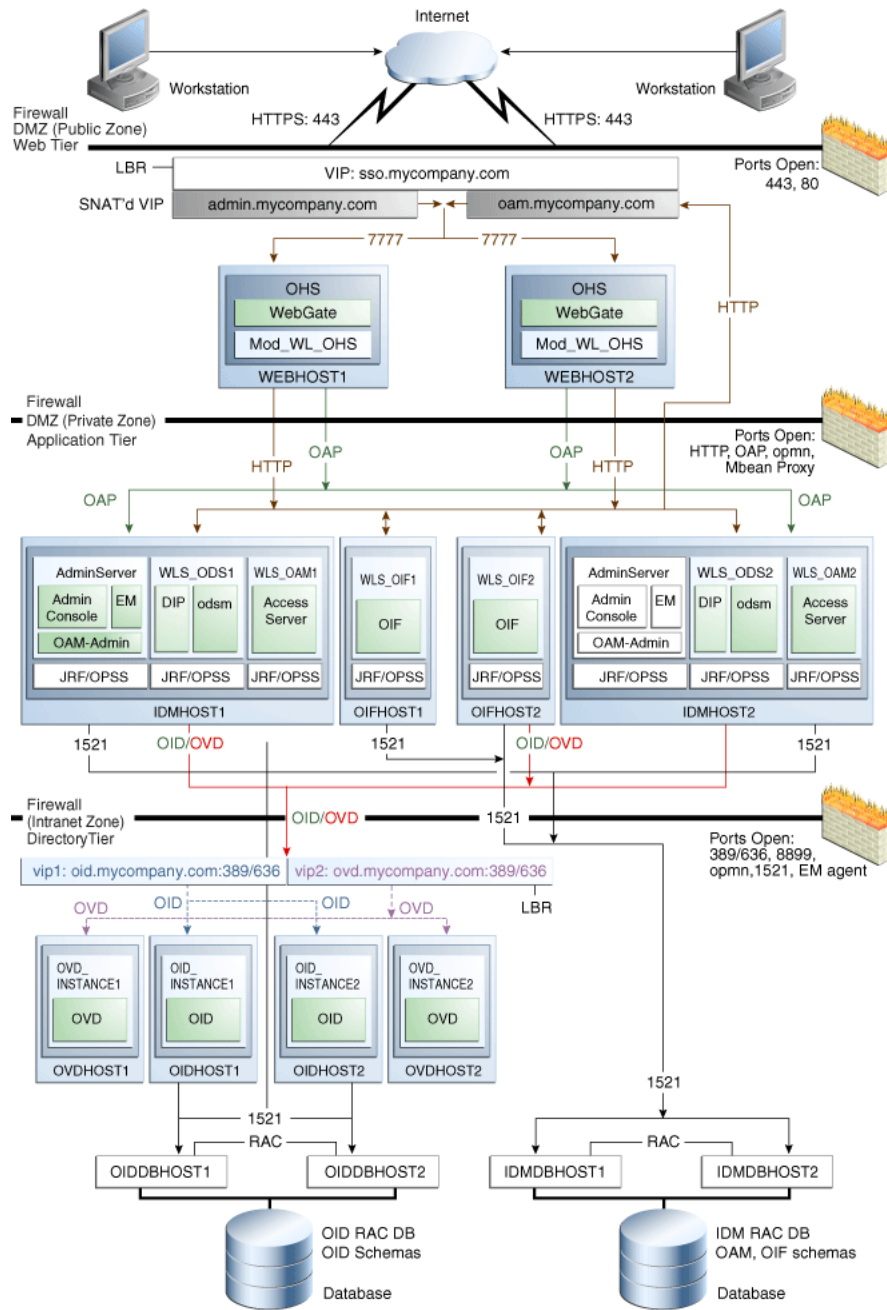
Security Provisions

The Oracle HTTP Servers process requests, received using the URL's sso.mycompany.com and admin.mycompany.com. admin.mycompany.com is a name only resolvable inside the firewall, and thus prevents access to sensitive resources such as the WebLogic console and Oracle Fusion Middleware console from the public domain.

1.4.5 Topology 5 - Oracle Identity Federation 11g

[Figure 1–5](#) is a diagram of the Oracle Identity Federation 11 topology.

Figure 1–5 Oracle Identity Federation 11g



1.4.5.1 Understanding the Directory Tier

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

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

- Oracle Internet Directory relies on RDBMS as its backend.

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

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

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

1.4.5.2 Understanding the Application Tier

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

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

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

In the application tier:

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

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

- `OIFHOST1` and `OIFHOST2` have the WebLogic Server with Oracle Identity Federation installed.
- On the firewall protecting the application tier, the HTTP ports, OIP port, and OAP port are open. The OIP (Oracle Identity Protocol) port is for the WebPass module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as querying user groups. The OAP (Oracle Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.

Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Service (OPSS) agent.
- The Administration Server, Oracle Enterprise Manager and Oracle Access Manager console are always bound to the listen address of the Administration Server.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Oracle Directory Integration Platform applications are targeted to the cluster.
- The WLS_OAM1 Managed Server on IDMHOST1 and WLS_OAM2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager and Access Manager applications are targeted to the cluster.
- The WLS_OIF1 Managed Server on OIFHOST1 and WLS_OIF2 Managed Server on OIFHOST2 are in a cluster and the Oracle Directory Services Manager and Access Manager applications are targeted to the cluster.
- Oracle Directory Services Manager and Oracle Directory Integration Platform are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.

High Availability Provisions

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

Security Provisions

Oracle WebLogic Console, Oracle Fusion Middleware Console and Oracle Access Manager Console are only accessible via admin.mycompany.com, which is only available inside the firewall.

1.4.5.3 Understanding the Web Tier

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

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

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

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Oracle Access Manager component), and the mod_wl_ohs plug-in module installed. The mod_wl_ohs plug-in module allows requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on IDMHOST1 and IDMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

Architecture Notes

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

Security Provisions

The Oracle HTTP Servers process requests, received using the URL's sso.mycompany.com and admin.mycompany.com. admin.mycompany.com is a name only resolvable inside the firewall, and thus prevents access to sensitive resources such as the WebLogic console and Oracle Fusion Middleware console from the public domain.

1.5 Using This Guide

If your enterprise deployment topology was created using the Oracle Identity Management Suite Release 11.1.1.2 binaries, follow the steps in the *Oracle Fusion Middleware Patching Guide* to upgrade your existing Oracle home to 11.1.1.3 before installing the Oracle Identity and Access Management Suite software. Once the software for the Oracle Identity and Access Management Suite is installed, follow the steps in this guide to extend your domain with the components required in your environment.

- To Extend your Domain with Oracle Authorization Policy Manager, refer to [Section 14.1, "Extending the Domain with Oracle Authorization Policy Manager"](#) in this guide
- To Extend your Domain with Oracle Identity Navigator, refer to [Section 14.2, "Extending the Domain with Oracle Identity Navigator"](#) in this guide
- To Extend your Domain with Oracle Access Manager 11g, refer to [Chapter 11, "Extending the Domain with Oracle Access Manager 11g"](#) in this guide
- To Extend your Domain with Oracle Adaptive Access Manager 11g, refer to [Chapter 12, "Extending the Domain with Oracle Adaptive Access Manager"](#) in this guide
- To Extend your Domain with Oracle Identity Manager 11g, refer to [Chapter 13, "Extending the Domain with Oracle Identity Manager"](#) in this guide
- To Extend your Domain with Oracle Identity Federation 11g refer to [Chapter 15, "Extending the Domain with Oracle Identity Federation"](#) in this guide

If you are creating an enterprise deployment topology from scratch, refer to the following sections of this guide in the order shown:

Topology	Steps required
Topology 1 - Oracle Access Manager 11g	<ul style="list-style-type: none"> Installing the Software Configuring the Database Repositories Configuring the Web Tier Creating the WebLogic Server Domain for Identity Management Extending the Domain with Oracle Internet Directory Extending the Domain with Oracle Virtual Directory Extending the Domain with Oracle Directory Integration Platform and ODSM Extending the Domain with Oracle Access Manager 11g Setting Up Node Manager
Topology 2 - Oracle Access Manager 10g and Oracle Identity Manager 11g	<ul style="list-style-type: none"> Installing the Software Configuring the Database Repositories Configuring the Web Tier Creating the WebLogic Server Domain for Identity Management Extending the Domain with Oracle Authorization Policy Manager Extending the Domain with Oracle Identity Navigator Extending the Domain with Oracle Internet Directory Extending the Domain with Oracle Virtual Directory Extending the Domain with Oracle Directory Integration Platform and ODSM Extending the Domain with Oracle Access Manager 10g Extending the Domain with Oracle Identity Manager Setting Up Node Manager

Topology	Steps required
Topology 3 - Oracle Access Manager 11g and Oracle Identity Manager 11g	<ul style="list-style-type: none"> Installing the Software Configuring the Database Repositories Configuring the Web Tier Creating the WebLogic Server Domain for Identity Management Extending the Domain with Oracle Authorization Policy Manager Extending the Domain with Oracle Identity Navigator Extending the Domain with Oracle Internet Directory Extending the Domain with Oracle Virtual Directory Extending the Domain with Oracle Directory Integration Platform and ODSM Extending the Domain with Oracle Access Manager 11g Extending the Domain with Oracle Identity Manager Setting Up Node Manager
Topology 4 - Oracle Adaptive Access Manager 11g	<ul style="list-style-type: none"> Installing the Software Configuring the Database Repositories Configuring the Web Tier Creating the WebLogic Server Domain for Identity Management Extending the Domain with Oracle Internet Directory Extending the Domain with Oracle Virtual Directory Extending the Domain with Oracle Directory Integration Platform and ODSM Extending the Domain with Oracle Access Manager 11g Extending the Domain with Oracle Adaptive Access Manager Extending the Domain with Oracle Identity Manager (Optional) Setting Up Node ManagerI

Topology	Steps required
Topology 5 - Oracle Identity Federation 11g	<ul style="list-style-type: none">Installing the SoftwareConfiguring the Database RepositoriesConfiguring the Web TierCreating the WebLogic Server Domain for Identity ManagementExtending the Domain with Oracle Identity NavigatorExtending the Domain with Oracle Internet DirectoryExtending the Domain with Oracle Virtual DirectoryExtending the Domain with Oracle Directory Integration Platform and ODSMExtending the Domain with Oracle Access Manager 11gExtending the Domain with Oracle Identity FederationSetting Up Node Manager

Prerequisites for Enterprise Deployments

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

This chapter includes the following topics:

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

2.1 Hardware Resource Planning

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

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

Table 2-1 Typical Hardware Requirements

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

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

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

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

2.2 Network Prerequisites

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

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

2.2.1 Load Balancers

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

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

- **Fault tolerant mode:** It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- **Other:** It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- **Sticky routing capability:** Ability to maintain sticky connections to components based on cookies or URL.
- **SSL acceleration** (this feature is recommended, but not required)
- **Configure the virtual server(s) in the load balancer for the directory tier with a high value for the connection timeout for TCP connections.** This value should be more than the maximum expected time over which no traffic is expected between the Oracle Access Manager and the directory tier.

2.2.2 Configuring Virtual Server Names and Ports on the Load Balancer

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

There are two load balancer devices in the recommended topologies. One load balancer is set up for external HTTP traffic and the other load balancer is set up for internal LDAP traffic. A deployment may choose to have a single load balancer device due to a variety of reasons. While this is supported, the deployment should consider the security implications of doing this and if found appropriate, open up the relevant firewall ports to allow traffic across the various DMZs. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant mode. The rest of this document assumes that the deployment is one of those shown in [Section 1.4, "The Enterprise Deployment Reference Topologies."](#)

oid.mycompany.com

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

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

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

- Monitor the heartbeat of the Oracle Internet Directory processes on OIHOST1 and OIHOST2. If an Oracle Internet Directory process stops on OIHOST1 or OIHOST2, or if either host OIHOST1 or OIHOST2 is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

ovd.mycompany.com

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

admin.mycompany.com

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

sso.mycompany.com

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

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

2.2.3 Administration Server Virtual IP Address

idmhost-vip.mycompany.com

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

2.2.4 Managing Oracle Fusion Middleware Component Connections

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

2.2.5 Oracle Access Manager Communication Protocol and Terminology

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

2.2.5.1 Oracle Access Manager Protocols

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

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

2.2.5.2 Overview of User Request

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

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

2.2.6 Firewall and Port Configuration

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

Most port numbers are assigned during installation.

[Table 2–2](#) lists the ports used in the Oracle Identity Management topologies, including the ports that you need to open on the firewalls in the topologies.

Firewall notation:

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

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

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Browser request	FW0	80	HTTP / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity Management.
Browser request	FW0	443	HTTPS / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity Management.
Oracle WebLogic Administration Server access from web tier	FW1	7001	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Enterprise Manager Agent - web tier to Enterprise Manager	FW1	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
Oracle HTTP Server to WLS_ODS	FW1	7006	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the <code>mod_weblogic</code> parameters used.
Oracle HTTP Server to WLS_OAM	FW1	14100	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the <code>mod_weblogic</code> parameters used.
Oracle HTTP Server to WLS_OAAM_ADMIN	FW1	14200	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the <code>mod_weblogic</code> parameters
Oracle HTTP Server to WLS_OAAM	FW1	14300	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the <code>mod_weblogic</code> parameters used.
Oracle Process Manager and Notification Server (OPMN) access in web tier	FW1	OPMN remote port	HTTP / Administration Server to OPMN	Outbound	N/A
Oracle HTTP Server proxy port	FW1	9999	HTTP / Administration Server to Oracle HTTP Server	Outbound	N/A
Access Server 10g access	FW1	6021	OAP	Both	N/A
Access Server 11g	FW1	5574-5575	OAP	Both	N/A
Oracle Coherence Port	FW1	9095	TCMP	Both	N/A

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

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

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

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
WebGate access from OAMADMINHOST	N/A	This is optional. You can use the listen port of the Oracle HTTP Server where the WebGate is configured (7777)	OAP	N/A	N/A
WebPass access from OAMADMINHOST	N/A	6022	OIP	N/A	N/A
Identity Server access	N/A	6022	OIP	N/A	N/A

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

2.3 WebLogic Domain Considerations

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

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

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

2.4 Shared Storage and Recommended Directory Structure

This following section details the directories and directory structure that Oracle recommends for an EDG topology. Other directory layouts are possible and supported, but the model adopted in this guide is chosen for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

2.4.1 Directory Structure Terminology and Environment Variables

This section describes directory structure terminology and environment variables.

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

- **MW_HOME:** This environment variable and related directory path refers to the location where Oracle Fusion Middleware resides. A MW_HOME has a WL_HOME, a ORACLE_COMMON_HOME and one or more ORACLE_HOMES.
- **WL_HOME:** This environment variable and related directory path contains installed files necessary to host a WebLogic Server.
- **ORACLE_HOME:** This environment variable and related directory path refers to the location where Oracle Fusion Middleware Identity Management is installed.
- **ORACLE_COMMON_HOME:** This environment variable and related directory path refers to the location where the Oracle Fusion Middleware Common Java Required Files (JRF) Libraries and Oracle Fusion Middleware Enterprise Manager Libraries are installed.
- **DOMAIN directory:** This directory path refers to the location where the Oracle WebLogic domain information (configuration artifacts) is stored. Different WebLogic Servers can use different domain directories even when in the same node as described [Section 2.4.2, "Recommended Locations for the Different Directories."](#)
- **ORACLE_INSTANCE:** An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. An Oracle instance directory contains updateable files, such as configuration files, log files, and temporary files.

2.4.2 Recommended Locations for the Different Directories

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

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

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

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

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

Table 2–3 Recommended Directory Structure

	Environment Variable	Mount Point or Directory Structure	Shared Storage Location	Hostname	Shared Storage
Common	ORACLE_BASE	/u01/app/oracle			
	MW_HOME	ORACLE_BASE/product/fmw			
Web Tier	ORACLE_HOME	MW_HOME/web			Optional
	ORACLE_INSTANCE	ORACLE_BASE/admin/instanceName			Optional
Identity Management Application Tier	MW_HOME	ORACLE_BASE/product/fmw	/vol/MW_HOME1	IDMHOST1	Yes
	MW_HOME	ORACLE_BASE/product/fmw	/vol/MW_HOME2	IDMHOST2	Yes
	ORACLE_HOME	MW_HOME/idm			Yes
	WL_HOME	MW_HOME/wlserver_version			Yes
	ORACLE_INSTANCE	ORACLE_BASE/admin/instanceName			Optional
	ASERVER_HOME	ORACLE_BASE/admin/domainName/aserver	/vol/admin	IDMHOST1	Yes
	ASERVER_DOMAIN_HOME	ASERVER_HOME/domainName			
	ASERVER_APP_HOME	ASERVER_HOME/applications			
	MSERVER_HOME	ORACLE_BASE/admin/domainName/mserver			Optional
	MSERVER_DOMAIN_HOME	MSERVER_HOME/domainName			
	MSERVER_APP_HOME	MSERVER_HOME/applications			
OAM Application Tier	OAM_BASE	MW_HOME/oam			Optional
	IDENTITY_SERVER_ORACLE_HOME	OAM_BASE/identity			Optional
	ACCESS_SERVER_ORACLE_HOME	OAM_BASE/access			Optional
	WEBPASS_ORACLE_HOME	OAM_BASE/webcomponents/identity			Optional
	POLICY_MANAGER_ORACLE_HOME	OAM_BASE/webcomponents/access			Optional
	WEBGATE_ORACLE_HOME	OAM_BASE/webgate			Optional
	Directory Tier	ORACLE_HOME	MW_HOME/idm		
ORACLE_INSTANCE		ORACLE_BASE/admin/instanceName			Optional

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

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

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

For Example:

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

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

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

For Example:

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

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

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

For Example:

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

Figure 2–1 shows the recommended directory structure.

Figure 2–1 Directory Structure for Identity Management

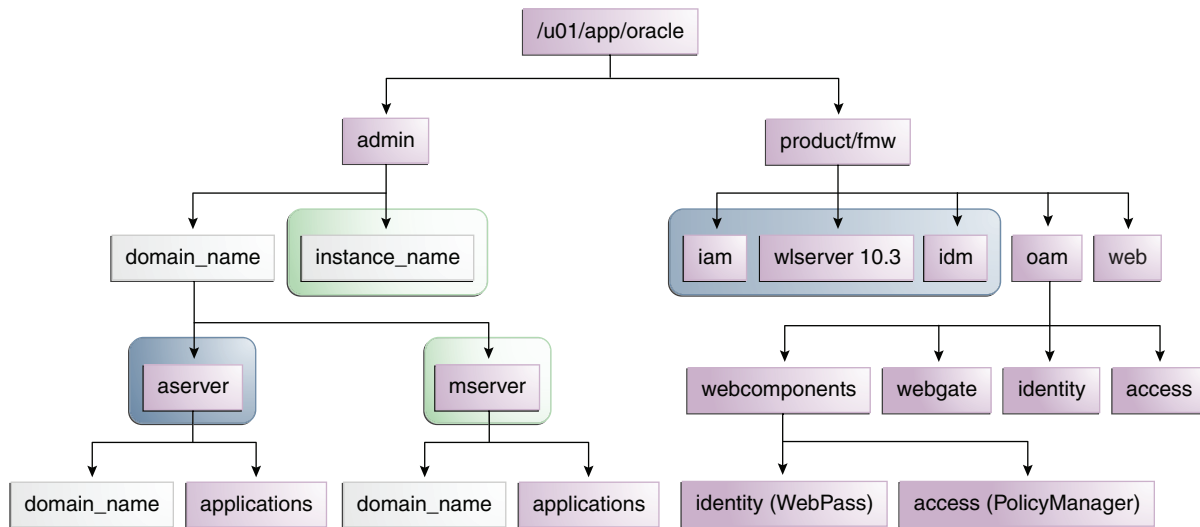






Table 2–4 explains what the color-coded elements in Figure 2–1 mean. The directory structure in Figure 2–1 does not show other required internal directories such as ORACLE_COMMON_HOME and jrockit.

Table 2–4 Directory Structure Elements

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

Configuring the Database Repositories

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

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

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

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

Databases Required

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

Table 3–1 Mapping between Topologies, Databases and Schemas

Topology Type	Database Names	Database Hosts	Service Names	Schemas in Database
OAM11g	INFRADB	INFRADBHOST1 INFRADBHOST2	idmedg.m ycompany.com	ODS
OAM11g	OAMDB	OAMDBHOST1 OAMDBHOST2	oamedg.m ycompany.com	OAM, IAU
OIM11g/OAM10g	INFRADB	INFRADBHOST1 INFRADBHOST2	idmedg.m ycompany.com	ODS
OIM11g/OAM10g	OIMDB	OIMDBHOST1 OIMDBHOST2	oimedg.m ycompany.com	OIM, MDS, SOAINFRA, ORASDPM

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

Topology Type	Database Names	Database Hosts	Service Names	Schemas in Database
OIM11g/OIM11g	INFRADB	INFRADBHOST1 INFRADBHOST2	idmedg.m ycompany.com, oamedg.m ycompany.com	ODS, OAM, IAU, APM, MDS
OIM11g/OIM11g	OIMDB	OIMDBHOST1 OIMDBHOST2	oimedg.m ycompany.com	OIM, MDS, SOAINFRA, ORASDPM
OIF11g/OAM11g	INFRADB	INFRADBHOST1 INFRADBHOST2	idmedg.m ycompany.com, oamedg.m ycompany.com	ODS, OAM, IAU
OIF11g/OAM11g	OIFDB	OIFDBHOST1 OIFDBHOST2	oifedg.m ycompany.com	OIF
OAAM11g/OAM11g	INFRADB	INFRADBHOST1 INFRADBHOST2	idmedg.m ycompany.com, oamedg.m ycompany.com	ODS, OAM, IAU
OAAM11g/OAM11g	OAAMDB	OAAMDBHOST1 OAAMDBHOST2	oaamedg.m mycompany.com	OAAM, OAAM_PARTN, MDS, IAU

Note:

- The SOA and OIM components share the MDS repository
- The MDS repository is for APM

The following sections apply to all the databases listed in [Table 3–1](#).

Database Versions Supported

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

http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

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

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

3.1 Real Application Clusters

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

Ideally the database will use Oracle ASM for the storage of data, however this is not necessary.

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

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

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

Install and configure the database repository as follows.

Oracle Clusterware

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

Automatic Storage Management

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

3.2 Configuring the Database for Oracle Fusion Middleware 11g Metadata

Create a Real Applications Clusters Database with the following characteristics:

- Database should 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 OIM reconciliation process.
- Database is created with ALT32UTF8 character set.
- In addition the database will have the following minimum initialization parameters defined:

Table 3–2 Minimum Initialization Parameters for Oracle RAC Database

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	400
session_max_open_files	50
sessions	500
processes	500
sga_target	512M
sga_max_size	800M
pga_aggregate_target	100M

Database Services

Oracle recommends using the Oracle Enterprise Manager Cluster Managed Services Page to create database services that client applications will use to connect to the database. For complete instructions on creating database services, see the chapter on Workload Management in the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*. A list of the services to be created can be found in Table 3–1. If possible, create one service per application, such as Oracle Identity Management and Oracle Access Manager.

You can also use SQL*Plus to configure your Oracle RAC database to automate failover for Oracle Internet Directory using the following instructions.

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

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

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

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

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

```
prompt> srvctl add service -d oam -s oam -r racnode1,racnode2
```

3. Start the service using srvctl:

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

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

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

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

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

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

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

3.3 Executing the Repository Creation Utility

Use the Repository Creation Utility (RCU) that is version compatible with the product you are installing. For example the Repository Creation utility for OID and OAM10g is different from the one for OAM11g and OAAM.

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

3.3.1 Procedure for Executing RCU

1. Start RCU by issuing this command:

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

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

Database Type: Oracle Database

- **Host Name:** Enter one of the Oracle RAC nodes. Specify the VIP name. For example: infradbhost1-vip.mycompany.com.
- **Port:** The port number for the database listener. For example: 1521
- **Service Name:** The service name of the database. For example idmedg.mycompany.com

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

Click **Next**.

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

Create a New Prefix: Enter a prefix to be added to the database schemas. Note that all schemas except for the ODS schema are required to have a prefix. For example, enter `EDG`.

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

Click **Next**.

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

- Be sure to install the correct schemas in the correct database.
 - You might have to run the RCU more than once to create all the schemas for a given topology.
 - [Table 3–1](#) in this chapter provides the recommended mapping between the schemas and their corresponding databases. Refer to this table to ensure that the correct details are entered in this screen.
 - The example at the end of the table illustrates these choices as well.
-
-

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. Oracle recommends choosing different passwords for different schema's to enhance security.
Click **Next**.
9. On the Map Tablespaces screen, accept the defaults and click **Next**.
10. On the Create Tablespaces screen, click **OK** to allow the creation of the tablespaces.
11. On the Creating tablespaces screen, click **OK** to acknowledge creation of the tablespaces.
12. On the Summary screen, the summary and verify that the details provided are accurate. Click **Create** to start the schema creation process.
13. On the Completion summary screen, verify that the schemas were created.
Click **Close** to exit.

3.3.2 RCU Example

This example illustrates the steps to create the required schemas in the INFRADB and OIMDB databases for the topology with OAM11g and OIM11g.

1. Start RCU as described in [Section 3.3.1, "Procedure for Executing RCU."](#)
2. On the Welcome Screen, click **Next**.
3. On the Connection Details screen, provide the details to connect to the INFRADB database running on INFRADBHOST1 and INFRADBHOST2. Enter the following values:
 - Host: `infradbhost1-vip.mycompany.com`
 - Port: 1521
 - Service Name: `idmedg.mycompany.com`
 - Username: `sys`
 - Password: `password`
 - Role: SYSDBAClick **Next**.
4. On the Select Components screen, select the appropriate schemas by referring to [Table 3-1](#). Select the ODS, OAM, IAU, APM, and MDS schemas. Click **Next**.
5. Follow the remaining steps in [Section 3.3.1, "Procedure for Executing RCU"](#) to create the schemas.
6. Verify that the schemas for the INFRADB database were successfully created.
7. Start RCU again to create the schemas for the OIMDB database.
8. On the Connection Details screen, provide the details to connect to the OIMDB database running on OIMDBHOST1 and OIMDBHOST2. Enter the following values:
 - Host: `oimdbhost1-vip.mycompany.com`
 - Port: 1521
 - Service Name: `oimedg.mycompany.com`
 - Username: `sys`
 - Password: `password`
 - Role: SYSDBAClick **Next**.
9. On the Select Components screen, select the appropriate schemas by referring to [Table 3-1](#). Select the OIM, MDS, SOAINFRA, and ORASDPM schemas on this screen.
10. Complete the schema creation by following the remaining steps in [Section 3.3.1, "Procedure for Executing RCU."](#)

Installing the Software

This chapter contains the following topics:

- [Section 4.1, "Introduction"](#)
- [Section 4.3, "Software Installation Summary"](#)
- [Section 4.4, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2"](#)
- [Section 4.5, "Installing Oracle Fusion Middleware"](#)
- [Section 4.6, "Upgrading the Oracle Homes for Oracle Identity Management Suite and Oracle SOA from 11.1.1.2 to 11.1.1.3"](#)
- [Section 4.7, "Patching the Software"](#)
- [Section 4.8, "Upgrading Existing Enterprise Deployment Topologies"](#)
- [Section 4.9, "Backing Up the Installation"](#)

4.1 Introduction

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

4.2 Using this Guide

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

The [Table 4–1](#) shows, for each topology, which software should be installed into each host.

The subsequent sections explain how to do this.

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

Where the two different pieces of Oracle binary software are installed onto the same host (for example OIM11g and OAM10g), this software will be installed in the same Middleware home location, but in different Oracle homes.

All software uses the same Middleware home location.

4.3 Software Installation Summary

Different topologies require different software to be installed. The installation process is the same for each product. Install the software shown in [Table 4-1](#) and [Table 4-2](#) for the desired topology, according to the instructions in this chapter

Table 4-1 Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	WLS	IAM	SOA	IDM	OAM 10g
All	WEBHOST1	X					
	WEBHOST2	X					
OAM11g	IDMHOST1		X	X			X
	IDMHOST2		X	X			X
	OIDHOST1						X
	OIDHOST2						X
	OVDHOST1						X
	OVDHOST2						X
OAAM11g	IDMHOST1		X	X			X
	IDMHOST2		X	X			X
	OAAMHOST1		X	X			
	OAAMHOST2		X	X			
	OIDHOST1						X
	OIDHOST2						X
	OVDHOST1						X
	OVDHOST2						X
OAM11g/OIM11g	IDMHOST1		X				X
	IDMHOST2		X				X
	OIMHOST1		X	X	X		X
	OIMHOST2		X	X	X		X
	OIDHOST1						X
	OIDHOST2						X
	OVDHOST1						X

Table 4–1 (Cont.) Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	WLS	IAM	SOA	IDM	OAM 10g
	OVDHOST2					X	
OAM10g/ OIM11g	IDMHOST1		X	X	X	X	
	IDMHOST2		X	X	X	X	
	OAMADMINHOST	X					X
	OAMHOST1						X
	OAMHOST2						X
	OIMHOST1		X	X	X	X	
	OIMHOST2		X	X	X	X	
	OIDHOST1						X
	OIDHOST2						X
	OVDHOST1						X
	OVDHOST2						
	OIF11g/OAM11g	IDMHOST1		X	X	X	X
IDMHOST2			X	X	X	X	
OIFHOST1			X	X	X	X	
OIFHOST2			X	X	X	X	
OIDHOST1							X
OIDHOST2							X
OVDHOST1							X
OVDHOST2							X

Table 4–2 Software Versions Used

Abbreviation	Product	Version
OHS11G	Oracle HTTP Server	11.1.1.3.0
WLS	Oracle WebLogic Server	10.3.3.0
IAM	Oracle Identity and Access Management Suite	11.1.1.3.0
SOA	Oracle SOA Suite	11.1.1.3.0
IDM	Oracle Identity Management Platform and Directory Services	11.1.1.3.0
OAM10g	Oracle Access Manager	10.1.4.3

Table 4–2 (Cont.) Software Versions Used

Abbreviation	Product	Version

Some of the topologies require two versions of the Identity Management software to be installed (see [Table 4–1](#)). In this scenario, the relevant Identity Management software is installed into separate Oracle homes.

4.4 Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2

This section explains how to install OHS.

4.4.1 Prerequisites

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

1. Ensure that the system, patch, kernel, and other requirements are met as specified in *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.
2. Ensure that port 777 is not in use, as described in [Section 4.4.1.1](#).
3. On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct, as described in [Section 4.4.1.2](#).

4.4.1.1 Check Port 7777

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

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

4.4.1.2 Check oraInst.loc

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

4.4.2 Installation

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

Start the Oracle Universal Installer as follows:

On UNIX, issue the command

```
runInstaller
```

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

Before Starting the install, ensure that the following environment variables are not set.

- LD_ASSUME_KERNEL
- ORACLE_INSTANCE

On the Specify Inventory Directory screen, do the following:

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

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

Click **OK**.

Proceed as follows:

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

Enter the OS group for the user performing the installation.

Click **Next**.

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

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

Click **Next**.

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

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

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

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

- Oracle Home Location Directory: `web`

6. On the Specify SecurityUpdates screen, choose whether or not to receive security updates from Oracle support.

Click **Next**.

7. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

On UNIX systems, when prompted, run the script `oracleRoot.sh` as the user `root`.

4.4.3 Upgrading Oracle HTTP Server from 11.1.1.2 to 11.1.1.3

Follow these steps to upgrade the OHS ORACLE_HOME from 11.1.1.2 to 11.1.1.3 on WEBHOST1 and WEBHOST2:

1. Start the WebTier Patchset Installer by running `./runInstaller`.
2. On the Welcome screen, click **Next**.
3. On the Prerequisite Checks screen, click **Next**.
4. On the Specify Install Location screen, provide the path to the Oracle Middleware home and the name of the Oracle home directory.
5. On the Installation Summary screen, validate your selections and click **Install**.

6. The Installation Progress screen shows the progress of the installation. Once the installation is complete, click **Next**.
7. On the Installation Complete Screen, click **Finish** to exit.

4.5 Installing Oracle Fusion Middleware

This section describes how to install Oracle Fusion Middleware.

4.5.1 Installing Oracle Fusion Middleware Components

This section describes how to install the required binaries to create the, Middleware home (`MW_HOME`), the Oracle WebLogic Server home (`WL_HOME`), the Oracle homes for the Identity Management Platform and Directory Services Suite Release 11.1.1.3.0 (`IDM_ORACLE_HOME`), the Oracle SOA Suite (`SOA_ORACLE_HOME`) and the Oracle Identity and Access Management Suite Release 11.1.1.3.0 (`IAM_ORACLE_HOME`). A summary of these homes is provided in [Table 4-3](#).

Table 4-3 Summary of Homes

Home Name	Home Description	Products Installed
<code>MW_HOME</code>	Consists of the Oracle WebLogic Server home and, optionally, one or more Oracle homes.	
<code>WL_HOME</code>	This is the root directory in which Oracle WebLogic Server is installed. The <code>WL_HOME</code> directory is a peer of Oracle home directory and resides with the <code>MW_HOME</code>	<ul style="list-style-type: none"> ▪ Oracle WebLogic Server 10.3.3.0
<code>IDM_ORACLE_HOME</code>	Contains the binary and library files for the Identity Management Platform and Directory Services Suite Release 11.1.1.3.0. Resides within the directory structure of the Middleware Home	<ul style="list-style-type: none"> ▪ Oracle Internet Directory ▪ Oracle Virtual Directory ▪ Oracle DIP ▪ ODSM ▪ OIF
<code>IAM_ORACLE_HOME</code>	Contains the binary and library files required for the Oracle Identity and Access Management Suite Release 11.1.1.3. Resides within the directory structure of the Middleware home	<ul style="list-style-type: none"> ▪ OAM ▪ OIM ▪ OAAM ▪ APM ▪ OIN
<code>SOA_ORACLE_HOME</code>	Contains the binary and library files required for the Oracle SOA Suite. Required only when creating topologies with OIM. Resides within the directory structure of the Middleware home.	<ul style="list-style-type: none"> ▪ SOA

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

4.5.2 Installing Oracle Fusion Middleware Home

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

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

1. Oracle WebLogic Server: [Section 4.5.3, "Installing Oracle WebLogic Server"](#)
2. One or more of the Oracle Fusion Middleware components
 - a. [Section 4.5.4, "Installing the Oracle Identity Management Platform and Directory Services Suite"](#)
 - b. [Section 4.5.5, "Installing the Oracle Identity and Access Management Suite"](#)
 - c. [Section 4.5.6, "Installing the Oracle SOA Suite"](#)
3. Oracle Fusion Middleware for Identity Management (see Section,

4.5.3 Installing Oracle WebLogic Server

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

The first step in the installation procedure is to install Oracle WebLogic Server. On UNIX/Linux, issue the command:

```
./wls_lin32.bin
```

On Windows, execute the command:

```
wls_win32.exe
```

Then proceed as follows.

1. On the Welcome screen, click **Next**.
2. On the Choose Middleware Home Directory screen, select **Create a New Middleware Home**.

For Middleware Home Directory, enter:

```
ORACLE_BASE/product/fmw.
```

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

Click **Next**.

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

Click **Next**.

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

Note: Oracle WebLogic Server and Oracle Coherence are installed.

Click **Next**.

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

- Middleware Home Directory: `ORACLE_BASE/product/fmw`
- Product Installation Directories for
 - WebLogic Server: `ORACLE_BASE/product/fmw/wlserver_10.3`
 - Oracle Coherence: `ORACLE_BASE/product/fmw/coherence_3.5`

Click **Next**.

6. On the Installation Summary screen, click **Next** to start the install process.
7. On the Installation complete screen, deselect **run Quickstart**.
Click **Done** to exit the WebLogic Server Installer.

4.5.4 Installing the Oracle Identity Management Platform and Directory Services Suite

Note: Because the installation is performed on shared storage, the two `MW_HOME` installations are accessible and used by the remaining servers in that tier of the topology.

When provisioning the software on the local hard disk of the machine, make sure to complete the steps on all the hosts in the tier.

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

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

```
HOST1> runInstaller
```

Then proceed as follows:

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

A dialog box appears with the following message:

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

Log in as root and run:

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

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

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

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

2. On the Welcome screen, click **Next**.
3. On the Select Installation Type screen, select **Install Software - Do Not Configure**, and then click **Next**.
4. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
5. On the Specify Installation Location screen, enter the following values:
 - Oracle Middleware Home: Select the previously installed Middleware home from the list for `MW_HOME`, for example
`/u01/app/oracle/product/fmw`
 - Oracle Home Directory: Enter `idm` as the Oracle home directory name.
 Click **Next**.
6. On the Specify Email for 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, click **Install**.
 When prompted, on Linux and UNIX installations, execute the script `oracleRoot.sh` as the root user.
8. On the Installation Progress screen, on Linux and UNIX systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the `oracleRoot.sh` script, as the root user.
9. On the Installation Complete screen, click **Finish**.

4.5.5 Installing the Oracle Identity and Access Management Suite

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

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

```
HOST1>./ runInstaller
```

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

```
/u01/app/product/fmw/jrockit_160_14_R27.6.5-32
```

Then perform these installation steps:

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

A dialog box appears with the following message:

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

Log in as root and run:

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

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

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

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

2. On the Welcome screen click **Next**.
3. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
4. On the Specify Installation Location screen, enter the following values:
 - **Oracle Middle Ware Home:** Select a previously installed Middleware Home from the drop-down list. For example: /u01/app/oracle/product/fmw
 - **Oracle Home Directory:** Enter iam" as the Oracle home directory name.Click **Next**.
5. On the Installation Summary screen, click **Install**.
6. On the Installation Complete screen, click **Finish**.

4.5.6 Installing the Oracle SOA Suite

Perform these steps to install the Oracle Identity Management Platform and Directory Services Suite on `IDMHOST1` and `IDMHOST2`.

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

Start the Oracle Fusion Middleware 11g SOA Suite Installer as follows:

```
HOST1>./ runInstaller
```

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

```
/u01/app/product/fmw/jrockit_160_14_R27.6.5-32.
```

Then perform these installation steps:

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

A dialog box appears with the following message:

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

Log in as root and run:

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

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

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

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

2. On the Welcome screen, click **Next**.
3. On the Prerequisite Checks screen, verify that the checks complete successfully, and then click **Next**.
4. On the Specify Installation Location screen, enter the following values:
 - **Oracle Middle Ware Home:** Select a previously installed Middleware Home from the drop-down list. For example: `/u01/app/oracle/product/fmw`

- **Oracle Home Directory:** Enter `soa` as the Oracle home directory name.
 - Click **Next**.
5. On the Installation Summary screen, click **Install**.
 6. On the Installation Complete screen, click **Finish**.

4.6 Upgrading the Oracle Homes for Oracle Identity Management Suite and Oracle SOA from 11.1.1.2 to 11.1.1.3

The Oracle homes for the Oracle Identity Management Suite 11.1.1.2 (`IDM_ORACLE_HOME`) and the Oracle SOA Suite (`SOA_ORACLE_HOME`) must be upgraded to Release 11.1.1.3 before creating the Identity Management domain. This section provides the steps to upgrade the `IDM_ORACLE_HOME` and the `SOA_ORACLE_HOME`.

4.6.1 Upgrading the Oracle Identity Management Platform and Directory Services Suite Oracle Home

Follow the steps in this section to upgrade the `IDM_ORACLE_HOME` from Release 11.1.1.2 to 11.1.1.3 using Oracle Universal Installer. Complete these step on `IDMHOST1` and `IDMHOST2`. Ensure that your machines meet all the prerequisites listed in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*. Start the Oracle Identity Management Patch Set installer as follows:

```
HOST1> ./runInstaller
```

Then proceed as follows

1. On the Welcome screen, click **Next**.
2. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
3. On the Specify Installation Location screen, enter the following values:
 - Oracle Middleware Home: Select the previously installed Middleware Home from the list, for example: `/u01/app/oracle/product/fmw`
 - Oracle Home Directory: Enter `idm` as the Oracle home directory. This Oracle home contains the Oracle Identity Management Suite binaries that will be upgraded from 11.1.1.2 to 11.1.1.3.

Click **Next**.
4. On the Specify Security Updates screen, enter these values:
 - Email Address: The email address for your My Oracle Support account.
 - Oracle Support Password: The password for your My Oracle Support account.

Select **I wish to receive security updates via My Oracle Support**.

Click **Next**.
5. On the Installation Summary screen, click **Install**. When prompted, on Linux and UNIX installations, execute the script `oracleRoot.sh` as the root user.
6. On the Installation Complete screen, click **Finish**.

4.6.2 Upgrading the Oracle SOA Suite Oracle Home

Follow the steps in this section to upgrade the `SOA_ORACLE_HOME` from release 11.1.1.2 to 11.1.1.3 using the Oracle SOA Suite Patch Set installer. Complete these step on `IDMHOST1` and `IDMHOST2`. Ensure that your machines meet all the prerequisites listed in the *Oracle Fusion Middleware Upgrade Guide for Oracle SOA Suite, WebCenter, and ADF*.

Start the Oracle SOA Suite Patch Set installer by typing:

```
HOST1> ./runInstaller
```

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

```
ORACLE_BASE/product/fmw/jrockit_160_14_R27.6.5-32
```

Then proceed as follows:

1. On the Welcome screen, click **Next**.
2. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
3. On the Specify Installation Location screen, enter the following Values:
 - Oracle Middleware Home: Select the previously installed Middleware Home from the drop-down list, for example: `/u01/app/oracle/product/fmw`.
 - Oracle Home Directory: Enter `soa` as the Oracle Home Directory. This Oracle home contains the Oracle SOA Suite binaries that will be upgraded from 11.1.1.2 to 11.1.1.3.

Click **Next**.

4. On the Installation Summary screen, click **Install**. When prompted, on Linux and UNIX installations, execute the script `oracleRoot.sh` as the root user.
5. On the Installation Complete screen, click **Finish**.

4.7 Patching the Software

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

4.7.1 Patch 9745107

Apply Patch 9745107 to all the WebLogic Homes in your environment by using the Oracle Smart Update utility. Follow these steps:

1. Change directory to the location of the Oracle Smart Update Utility located under the `MW_HOME/utills/bsu` directory

```
IDMHOST1 > cd $MW_HOME/utills/bsu
```

2. Start the Oracle Smart Update Utility by running `bsu.sh`.

```
IDMHOST1 > ./bsu.sh
```

3. Log in to Oracle Smart Update with your support ID and password to download the patches.

4. After the utility validates your credentials, the Register Security Updates screen appears. 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 **Continue**.

5. Select your Target Installation in the right pane and click **Get Patches**.
6. Select **Patches** then **Retrieve Private**. View Private Patch appears.
7. Provide the **Patch Identifier** and the **Passcode** for the patch and click **Download**. For Patch 9745107, the patch identifier is **3SAY** and the passcode is **1IN3XNGX**.
8. Select **Yes**, then enable **Check for Conflicts** to enable the Oracle Smart Update to check for conflicts.

Click **OK**.
9. After Oracle Smart Update validates that there are no conflicts, click **OK** to download the patch
10. Click the **Manage Patches** tab.
11. Select the patch with the Patch ID 3SAY from the downloaded patches and click **Apply**.
12. The following message appears:

Temporary patches for Oracle products provided through this tool are developed by Oracle in response to issues reported when using Oracle products in certain scenarios. Oracle testing of patches is typically limited to validation that the patch addresses the specific issue reported. This scope of testing is more limited than the testing performed on product version releases and maintenance packs. Oracle only recommends the use of patches for resolving specific issues that have been encountered in the user environment, or are likely to be encountered. Oracle recommends that users perform functional testing of their environments after applying temporary patches.

Click **OK** to continue.

13. A Module Patch Warning appears with the message:

You are attempting to apply a patch for a module applicable to multiple products on the same system. Do you like to Continue.

Click **Yes**

14. The Oracle Smart Update validates the patch. After the validation is complete, click **OK** to install the patch

4.7.2 Patch 9449855

Download the Patch 9449855 from My Oracle Support at <https://support.oracle.com>. Patch all the common Oracle homes in your environment with this patch. Make sure that your environment meets the prerequisites listed in the Readme file that is shipped with the patch. Follow these steps to apply the patch:

1. Unzip the patch to a directory on your machine by using `unzip`. For example:

```
unzip p9449855_111130_Generic.zip.
```

This creates a directory called 9449855.

2. Set the Oracle home to the common Oracle home. For example:

```
export ORACLE_HOME=$MW_HOME/oracle_common
```

3. Set the path to include the OPatch directory under the Oracle home. For example:

```
export PATH=$ORACLE_HOME/OPatch:$PATH
```

4. Navigate to the directory to the directory where the patch is located. For Example:

```
cd 9449855
```

5. Apply the patch using `opatch apply`. The output should be similar to the following:

```
[Prompt> opatch apply
Invoking OPatch 11.1.0.8.0
Oracle Interim Patch Installer version 11.1.0.8.0
Copyright (c) 2009, Oracle Corporation. All rights reserved.
```

```
Oracle Home      : /u01/app/oracle/product/fmw/oracle_common
Central Inventory : /u01/app/oraInventory
                  from   : /etc/oraInst.loc
OPatch version   : 11.1.0.8.0
OUI version      : 11.1.0.8.0
OUI location     : /u01/app/oracle/product/fmw/oracle_common/oui
Log file location : /u01/app/oracle/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch2010-06-11_17-08-43PM.log
```

```
Patch history file: /u01/app/oracle/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch_history.txt
```

```
OPatch detects the Middleware Home as "/u01/app/oracle/plus/product/fmw"
```

```
ApplySession applying interim patch '9449855' to OH
'/u01/app/oracle/product/fmw/oracle_common'
```

```
Running prerequisite checks...
```

```
OPatch detected non-cluster Oracle Home from the inventory and will patch the
local system only.
```

```
Backing up files and inventory (not for auto-rollback) for the Oracle Home
Backing up files affected by the patch '9449855' for restore. This might take a
while...
```

```
Backing up files affected by the patch '9449855' for rollback. This might take
a while...
```

```
Patching component oracle.jrf.opss, 11.1.1.3.0...
Copying file to /u01/app/oracle/product/fmw/oracle_
common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar"
Copying file to /u01/app/oracle/product/fmw/oracle_
common/common/wlst/resources/oamAuthnProvider.jar"
ApplySession adding interim patch '9449855' to inventory
```

```
Verifying the update...
```

```
Inventory check OK: Patch ID 9449855 is registered in Oracle Home inventory
```

with proper meta-data.
Files check OK: Files from Patch ID 9449855 are present in Oracle Home.

6. Validate that the patch applied successfully by running `opatch lsinventory`. The output is similar to this

```
Prompt> opatch apply
Invoking OPatch 11.1.0.8.0

Oracle Interim Patch Installer version 11.1.0.8.0
Copyright (c) 2009, Oracle Corporation. All rights reserved.

Oracle Home      : /u01/app/oracle/plus/product/fmw/oracle_common
Central Inventory : /u01/app/oraInventory
   from           : /etc/oraInst.loc
OPatch version   : 11.1.0.8.0
OUI version      : 11.1.0.8.0
OUI location     : /u01/app/oracle/plus/product/fmw/oracle_common/oui
Log file location : /u01/app/oracle/plus/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch2010-06-11_17-08-43PM.log

Patch history file: /u01/app/oracle/plus/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch_history.txt

OPatch detects the Middleware Home as "/u01/app/oracle/plus/product/fmw"

ApplySession applying interim patch '9449855' to OH
'/u01/app/oracle/plus/product/fmw/oracle_common'

Running prerequisite checks...

OPatch detected non-cluster Oracle Home from the inventory and will patch the
local system only.

Backing up files and inventory (not for auto-rollback) for the Oracle Home
Backing up files affected by the patch '9449855' for restore. This might take a
while...
Backing up files affected by the patch '9449855' for rollback. This might take
a while...

Patching component oracle.jrf.opss, 11.1.1.3.0...
Copying file to "/u01/app/oracle/plus/product/fmw/oracle_
common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar"
Copying file to "/u01/app/oracle/plus/product/fmw/oracle_
common/common/wlst/resources/oamAuthnProvider.jar"
ApplySession adding interim patch '9449855' to inventory

Verifying the update...
Inventory check OK: Patch ID 9449855 is registered in Oracle Home inventory
with proper meta-data.

Files check OK: Files from Patch ID 9449855 are present in Oracle Home.

OPatch succeeded.

[Prompt> opatch lsinventory
Invoking OPatch 11.1.0.8.0

Oracle Interim Patch Installer version 11.1.0.8.0
```

```
Copyright (c) 2009, Oracle Corporation. All rights reserved.
Oracle Home       : /u01/app/oracle/plus/product/fmw/oracle_common
```

```
Central Inventory : /u01/app/oraInventory
  from            : /etc/oraInst.loc
OPatch version    : 11.1.0.8.0
OUI version       : 11.1.0.8.0
OUI location      : /u01/app/oracle/plus/product/fmw/oracle_common/oui
Log file location : /u01/app/oracle/plus/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch2010-06-11_17-28-59PM.log
```

```
Patch history file: /u01/app/oracle/plus/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch_history.txt
```

```
OPatch detects the Middleware Home as "/u01/app/oracle/plus/product/fmw"
```

```
Lsinventory Output file location : /u01/app/oracle/plus/product/fmw/oracle_
common/cfgtoollogs/opatch/lsinv/lsinventory2010-06-11_17-28-59PM.txt
```

```
-----
Installed Top-level Products (2):
```

```
Application Server 11g SOA Patchset
                                11.1.1.3.0
Oracle AS Common Toplevel Component
                                11.1.1.2.0
There are 2 products installed in this Oracle Home.
```

```
Interim patches (1) :
```

```
Patch 9449855      : applied on Fri Jun 11 17:08:54 PDT 2010
Unique Patch ID: 12621969
  Created on 19 May 2010, 21:47:40 hrs US/Pacific
  Bugs fixed:
    9449855
```

4.7.3 Patch 9824531

Download Patch 9824531 from My Oracle Support at <https://support.oracle.com>. Patch all the common Oracle homes in your environment with this patch. Make sure that your environment meets the prerequisites listed in the Readme file that is shipped with the patch. Follow these steps to apply the patch:

1. Unzip the patch. This creates a directory called 9824531.
2. Set your Oracle home to the Oracle common home and make sure that the `ORACLE_HOME/OPatch` directory is in your path.
3. Navigate to the 9824531 directory.
4. Apply the patch using the `opatch apply` command.
5. Answer Y when you see the question Is the local system ready for patching? [y|n].

Example:

```
export ORACLE_HOME=MW_HOME/oracle_common
export PATH=$ORACLE_HOME/OPatch:$PATH
prompt> cd 9824531
prompt> opatch apply -jdk /u01/app/oracle/product/fmw/jdk160_18
```

The output looks similar to this:

```
Prompt> opatch apply -jdk /u01/app/oracle/product/fmw/jdk160_18
Invoking OPatch 11.1.0.8.0
```

```
Oracle Interim Patch Installer version 11.1.0.8.0
Copyright (c) 2009, Oracle Corporation. All rights reserved.
```

```
Oracle Home      : /u01/app/oracle/product/fmw/oracle_common
Central Inventory : /u01/app/oraInventory
   from           : /etc/oraInst.loc
OPatch version   : 11.1.0.8.0
OUI version      : 11.1.0.8.0
OUI location     : /u01/app/oracle/product/fmw/oracle_common/oui
Log file location : /u01/app/oracle/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch2010-06-24_18-26-07PM.log
```

```
Patch history file: /u01/app/oracle/product/fmw/oracle_
common/cfgtoollogs/opatch/opatch_history.txt
```

```
OPatch detects the Middleware Home as "/u01/app/oracle/product/fmw"
```

```
ApplySession applying interim patch '9824531' to OH
'/u01/app/oracle/product/fmw/oracle_common'
```

```
Running prerequisite checks...
```

```
OPatch detected non-cluster Oracle Home from the inventory and will patch the
local system only.
```

```
Please shutdown Oracle instances running out of this ORACLE_HOME on the local
system.
```

```
(Oracle Home = '/u01/app/oracle/product/fmw/oracle_common')
```

```
Is the local system ready for patching? [y|n]
```

```
Y
```

```
User Responded with: Y
```

```
Backing up files and inventory (not for auto-rollback) for the Oracle Home
Backing up files affected by the patch '9824531' for restore. This might take a
while...
```

```
Backing up files affected by the patch '9824531' for rollback. This might take a
while...
```

```
Patching component oracle.jrf.adf.rt, 11.1.1.3.0...
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.model_11.1.1/adfm.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.model_11.1.1/adf.oracle.domain.ear"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/adf.oracle.domain.webapp.war"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/adf-faces-databinding-rt.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/oracle-page-templates.jar"
```

```

Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.share_11.1.1/adf-share-support.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_common/modules/oracle.mds_
11.1.1/mdsrt.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/dvt-faces.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/dvt-utils.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/dvt-trinidad.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/dvt-jclient.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/trinidad-api.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/trinidad-impl.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/adf-richclient-api-11.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/adf-richclient-impl-11.jar"
Copying file to "/u01/app/oracle/product/fmw/oracle_
common/modules/oracle.adf.view_11.1.1/adf-richclient-automation-11.jar"
ApplySession adding interim patch '9824531' to inventory

```

Verifying the update...

Inventory check OK: Patch ID 9824531 is registered in Oracle Home inventory with proper meta-data.

Files check OK: Files from Patch ID 9824531 are present in Oracle Home.

The local system has been patched and can be restarted.

OPatch succeeded.

4.7.4 Patch 9477292

Download Patch 9477292 from My Oracle Support at <https://support.oracle.com>. Patch all the IDM Oracle homes in your environment with this patch. Make sure that your environment meets the prerequisites listed in the Readme file that is shipped with the patch. Follow these steps to apply the patch:

1. Unzip the patch, this creates a directory called 9477292.
2. Shut down all services running from the *IDM_ORACLE_HOME*.
3. Set your *ORACLE_HOME* to the *IDM_ORACLE_HOME* and make sure that the *ORACLE_HOME/OPatch* directory is in your path.
4. Navigate to the 9477292 directory.
5. Apply the patch using the `opatch apply` command.
6. Answer Y when you see the question Is the local system ready for patching? [y|n].

Example:

```

Prompt> opatch apply
Invoking OPatch 11.1.0.8.0
Oracle Interim Patch Installer version 11.1.0.8.0
Copyright (c) 2009, Oracle Corporation. All rights reserved.

```

```

Oracle Home      : /u01/app/oracle/product/fmw/idm
Central Inventory : /u01/app/oraInventory
    from         : /etc/oraInst.loc
OPatch version   : 11.1.0.8.0
OUI version      : 11.1.0.8.0
OUI location     : /u01/app/oracle/product/fmw/idm/oui
Log file location :
/u01/app/oracle/product/fmw/idm/cfgtoollogs/patch/patch2010-07-18_
11-49-02AM.log
Patch history file: /u01/app/oracle/product/fmw/idm/cfgtoollogs/patch/patch_
history.txt
OPatch detects the Middleware Home as "/u01/app/oracle/product/fmw"
ApplySession applying interim patch '9477292' to OH
'/u01/app/oracle/product/fmw/idm'
Running prerequisite checks...
OPatch detected non-cluster Oracle Home from the inventory and will patch the
local system only.
Please shutdown Oracle instances running out of this ORACLE_HOME on the local
system.
(Oracle Home = '/u01/app/oracle/product/fmw/idm')
Is the local system ready for patching? [y|n]
Y
User Responded with: Y
Backing up files and inventory (not for auto-rollback) for the Oracle Home
Backing up files affected by the patch '9477292' for restore. This might take a
while...
Backing up files affected by the patch '9477292' for rollback. This might take
a while...
Patching component oracle.as.im.install, 11.1.1.3.0...
Copying file to "/u01/app/oracle/product/fmw/idm/install/config/StartUtil.dll"
Copying file to
"/u01/app/oracle/product/fmw/idm/install/config/StartUtil64.dll"
Copying file to "/u01/app/oracle/product/fmw/idm/install/config/ASConfig.jar"
Copying file to
"/u01/app/oracle/product/fmw/idm/inventory/Scripts/ext/jlib/engine.jar"
Copying file to
"/u01/app/oracle/product/fmw/idm/inventory/Scripts/ext/jlib/im/im.jar"
ApplySession adding interim patch '9477292' to inventory

Verifying the update...
Inventory check OK: Patch ID 9477292 is registered in Oracle Home inventory
with proper meta-data.
Files check OK: Files from Patch ID 9477292 are present in Oracle Home.
The local system has been patched and can be restarted.
OPatch succeeded.

```

7. Validate that the patch applied successfully by running `opatch lsinventory`. The output is similar to this:

```

Prompt> opatch lsinventory
Invoking OPatch 11.1.0.8.0

Oracle Interim Patch Installer version 11.1.0.8.0
Copyright (c) 2009, Oracle Corporation. All rights reserved.

Oracle Home      : /u01/app/oracle/product/fmw/idm
Central Inventory : /u01/app/oraInventory
    from         : /etc/oraInst.loc
OPatch version   : 11.1.0.8.0
OUI version      : 11.1.0.8.0

```



```
OUI location      : /u01/app/oracle/product/fmw/idm/oui
Log file location :
/u01/app/oracle/product/fmw/idm/cfgtoollogs/patch/patch2010-07-18_
11-52-02AM.log

Patch history file: /u01/app/oracle/product/fmw/idm/cfgtoollogs/patch/patch_
history.txt
```

```
OPatch detects the Middleware Home as "/u01/app/oracle/product/fmw"
```

```
Lsinventory Output file location :
/u01/app/oracle/product/fmw/idm/cfgtoollogs/patch/lsinv/lsinventory2010-07-18_
11-52-02AM.txt
```

```
-----
-
Installed Top-level Products (2):
```

```
Oracle Identity Management 11g                11.1.1.2.0
Oracle Identity Management 11g Patchset       11.1.1.3.0
There are 2 products installed in this Oracle Home.
```

```
Interim patches (9) :
```

```
Patch 9477292      : applied on Sun Jul 18 11:50:03 PDT 2010
Unique Patch ID: 12767997
Created on 15 Jul 2010, 14:41:36 hrs US/Pacific
Bugs fixed:
9477292
```

```
Patch 7663342      : applied on Thu Jun 10 19:24:50 PDT 2010
Created on 15 Jan 2009, 00:17:30 hrs PST8PDT
Bugs fixed:
7663342
```

```
Patch 7572595      : applied on Thu Jun 10 19:24:24 PDT 2010
Created on 15 Jan 2009, 02:37:01 hrs PST8PDT
Bugs fixed:
7572595
```

```
Patch 6599470      : applied on Thu Jun 10 19:24:09 PDT 2010
Created on 21 Jan 2009, 01:50:17 hrs PST8PDT
Bugs fixed:
6599470
```

```
Patch 7707476      : applied on Thu Jun 10 19:23:55 PDT 2010
Created on 10 Feb 2009, 19:13:18 hrs PST8PDT
Bugs fixed:
7707476, 7360273, 7284982
```

```
Patch 7393921      : applied on Thu Jun 10 19:22:37 PDT 2010
Created on 17 Oct 2008, 03:32:19 hrs PST8PDT
Bugs fixed:
7393921
```

```
Patch 6750400      : applied on Thu Jun 10 19:21:42 PDT 2010
Created on 3 Nov 2008, 22:33:54 hrs PST8PDT
Bugs fixed:
```

6750400

Patch 7427144 : applied on Thu Jun 10 19:21:00 PDT 2010
Created on 29 Oct 2008, 00:14:14 hrs PST8PDT
Bugs fixed:
7427144

Patch 6845838 : applied on Thu Jun 10 19:20:52 PDT 2010
Created on 3 Nov 2008, 22:00:04 hrs PST8PDT
Bugs fixed:
6845838

-
OPatch succeeded.

4.7.5 Creating the wlfullclient.jar File

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

1. Navigate to the `MW_HOME/wlserver_10.3/server/lib` directory
2. Set your `JAVA_HOME` to `MW_HOME/jdk160_18` and ensure that your `JAVA_HOME/bin` directory is in your path.
3. Create the `wlfullclient.jar` file by running:

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

4.7.6 Provisioning the Oracle Identity Manager Login Modules Under the WebLogic Server Library Directory

Due to issues with versions of the configuration wizard, some environmental variables are not added to the `setDomain.env` script. This causes certain install sequences to fail. This section is a temporary workaround for that problem.

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

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

```
cp $IAM_ORACLE_HOME/server/loginmodule/wls/* $MW_HOME/wlserver_10.3/server/lib/mbeantypes/.
```
2. Change directory to `MW_HOME/wlserver_10.3/server/lib/mbeantypes/`.

```
cd $MW_HOME/wlserver_10.3/server/lib/mbeantypes
```
3. Change the permissions on these files to 750 by using the `chmod` command.

```
chmod 750 *
```

4.7.7 Patch 9847606

Download Patch 9847606 from My Oracle Support at <https://support.oracle.com>. Patch all the Middleware homes in your environment with this patch. Make sure that your environment meets the prerequisites listed in the Readme file that is shipped with the patch.

Follow these steps to apply the patch:

1. Shut down any managed servers that are running.

```
cd MW_HOME
```

2. Make a backup of the original JRockit JDK.

```
mv jrockit_160_17_R28.0.0-679 jrockit_160_17_R28.0.0-679.orig
```

3. Unzip the patch.

```
unzip p9847606_2801_LINUX.zip
```

4. Rename the patched jdk to the original name.

```
mv jrockit-jdk1.6.0_20 jrockit_160_17_R28.0.0-679
```

5. Restart Managed Servers as necessary.

4.8 Upgrading Existing Enterprise Deployment Topologies

If your enterprise deployment topology was created using the Oracle Identity Management Suite Release 11.1.1.2 binaries, follow the steps in the *Oracle Fusion Middleware Patching Guide* to upgrade your existing Oracle home to 11.1.1.3 before installing the Oracle Identity and Access Management Suite software.

4.9 Backing Up the Installation

Once you have created the Fusion Middleware home, stop all servers and back up the Fusion Middleware home. Type:

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

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

Configuring the Web Tier

This chapter describes how to configure the Oracle Web Tier.

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

This chapter includes the following topics:

- [Section 5.1, "Configuring the Web Tier"](#)
- [Section 5.2, "Configuring the Oracle Web Tier"](#)
- [Section 5.3, "Configuring Oracle HTTP Server with the Load Balancer"](#)
- [Section 5.4, "Configuring Virtual Hosts"](#)
- [Section 5.5, "Validating the Installation"](#)

5.1 Configuring the Web Tier

This chapter describes how to configure the Oracle Web Tier.

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

Prior to configuring the Oracle Web Tier software must have been installed on WEBHOST1 and WEBHOST2 as described in [Chapter 4, "Installing the Software."](#)

5.2 Configuring the Oracle Web Tier

The steps for configuring the Oracle Web Tier are the same for both webhost1 and webhost2.

Perform these steps to configure the Oracle web tier:

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

```
WEBHOST1> cd ORACLE_HOME/bin
```

2. Start the Configuration Wizard:

```
WEBHOST1> ./config.sh
```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

Ensure that Associate Selected Components with WebLogic Domain is not selected.

Ensure Oracle Web Cache is NOT selected.

Click **Next**.

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

Enter the following values for WEBHOST1:

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

Enter the following values for WEBHOST2:

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

Click **Next**.

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

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

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

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

5. On the Specify Security Updates screen, specify these values:

- **Email Address:** The email address for your My Oracle Support account.
- **Oracle Support Password:** The password for your My Oracle Support account.

Select: **I wish to receive security updates via My Oracle Support.**

Click **Next**.

6. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

Click **Install**.

On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

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

5.2.1 Validating the Installation

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

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

5.3 Configuring Oracle HTTP Server with the Load Balancer

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server, that is, `WEBHOST1` and `WEBHOST`.

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

Also, set Monitors for HTTP.

5.4 Configuring Virtual Hosts

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

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

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

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

5.5 Validating the Installation

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

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

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

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

Creating the WebLogic Server Domain for Identity Management

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

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

This chapter contains the following sections.

- [Section 6.1, "Enabling ADMINVHN on IDMHOST1"](#)
- [Section 6.2, "Running the Configuration Wizard on IDMHOST1 to Create a Domain"](#)
- [Section 6.3, "Creating boot.properties for the Administration Server on IDMHOST1"](#)
- [Section 6.4, "Starting Node Manager on IDMHOST1"](#)
- [Section 6.5, "Updating the Node Manager Credentials"](#)
- [Section 6.6, "Disabling Host Name Verification for the Oracle WebLogic Administration Server"](#)
- [Section 6.7, "Stopping and Starting the WebLogic Administration Server"](#)
- [Section 6.8, "Validating the Administration Server"](#)
- [Section 6.9, "Configuring Oracle HTTP Server for the Administration Server"](#)
- [Section 6.11, "Setting the Front End URL for the Administration Console"](#)
- [Section 6.12, "Validating Access Through Oracle HTTP Server"](#)
- [Section 6.13, "Manually Failing Over the Administration Server"](#)
- [Section 6.14, "Backing Up the Installation"](#)

6.1 Enabling ADMINVHN on IDMHOST1

Note that this step is required for failover of the Administration Server, regardless of whether other Oracle Fusion Middleware components are installed later or not.

You will associate the Administration Server with a virtual IP address, `ADMINVHN.mycompany.com`. Check that `ADMINVHN.mycompany.com` is enabled on IDMHOST1.

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

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

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

For example:

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

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

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

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

```
/bin/ping 100.200.140.206
```

6.2 Running the Configuration Wizard on IDMHOST1 to Create a Domain

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

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

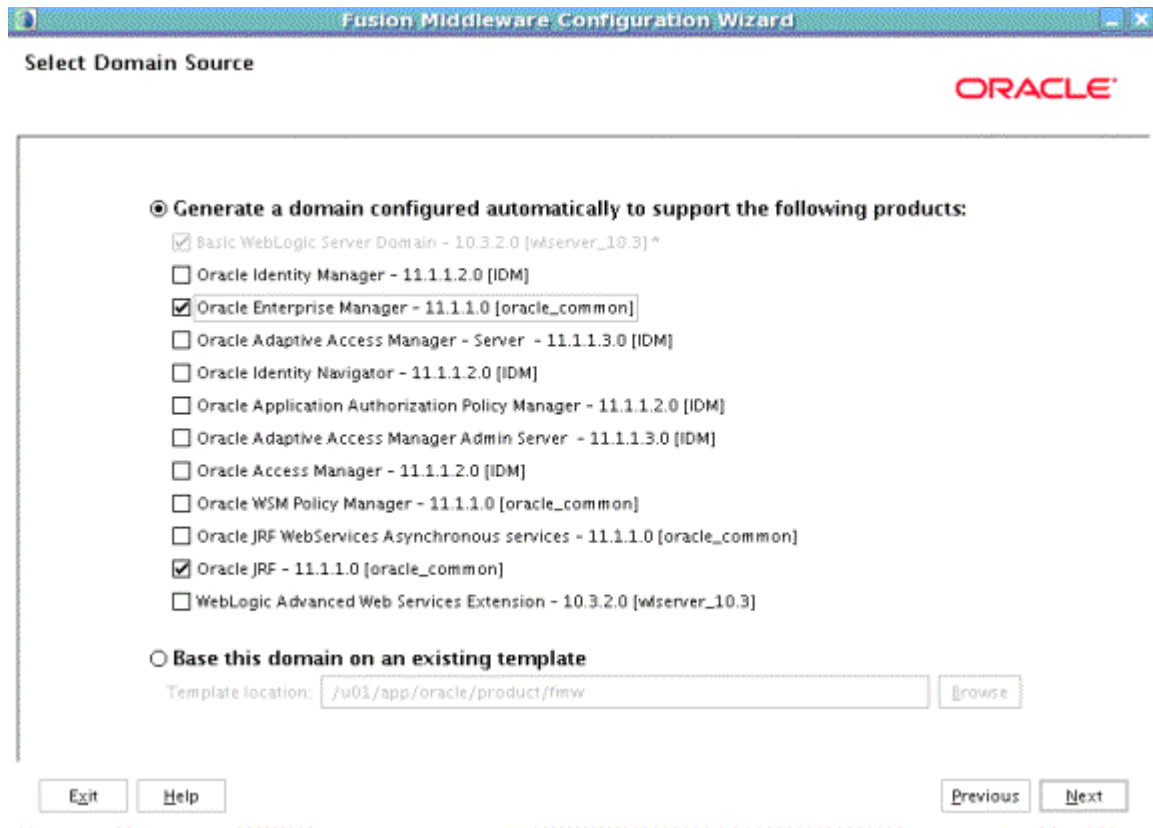
```
IDMHOST1> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
```

2. Start the Oracle Fusion Middleware Configuration Wizard:

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

3. On the Welcome screen, select Create a New WebLogic Domain, and click **Next**.
4. The Select Domain Source screen is displayed in [Figure 6-1](#).

Figure 6–1 Select Domain Source Screen



On the Select Domain Source screen, do the following:

- Select **Generate a domain configured automatically to support the following products**.
- Select the following products:
 - **Basic WebLogic Server Domain - 10.3.3.0 [wlserver_10.3]** (This should be selected automatically.)
 - **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**
 - **Oracle JRF - 11.1.1.0 [oracle_common]** (This should be selected automatically.)

Click **Next**.

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

Make sure that the domain directory matches the directory and shared storage mount point recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

Enter

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

for the domain directory and

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

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

6. Click **Next**.
7. On the Configure Administrator Username and Password screen, enter the username (default is `weblogic`) and password to be used for the domain's administrator. For example:
 - **Name:** `weblogic`
 - **User Password:** `password for weblogic user`
 - **Confirm User Password:** `password for weblogic user`
 - **Description:** `This user is the default administrator.`Click **Next**.
8. On the Configure Server Start Mode and JDK screen, do the following:
 - For WebLogic Domain Startup Mode, select **Production Mode**.
 - For JDK Selection, select **JROCKIT SDK1.6.0_14**Click **Next**.
9. On the Select Optional Configuration screen, select the following:
 - **Administration Server**
 - **Managed Servers, Clusters and Machines**Click **Next**.
10. On the Configure the Administration Server screen, enter the following values:
 - **Name:** **AdminServer**
 - **Listen Address:** **ADMINVHN.mycompany.com.**
 - **Listen Port:** **7001**
 - **SSL listen port:** **N/A**
 - **SSL enabled:** uncheckedClick **Next**.
11. On the Configure Managed Servers screen, click **Next**
12. On the Configure Clusters screen, click **Next**
13. On the Configure Machines screen, click the **Unix Machine** tab and then click **Add** to add the following machine. The machine name does not need to be a valid hostname or listen address, it is just a unique identifier of a nodemanager location:
 - **Name:** `ADMINHOST`
 - **Node manager listen address:** `localhost`Leave all other fields to their default values.
14. Click **Next**.
15. On the Assign Servers to Machines screen, assign servers to machines as follows:
 - **ADMINHOST:** **AdminServer**Click **Next**.
16. On the Configuration Summary screen, validate that your choices are correct, then click **Create**.

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

6.3 Creating boot.properties for the Administration Server on IDMHOST1

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

For the Administration Server:

1. Create the following directory structure:

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

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

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

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

6.4 Starting Node Manager on IDMHOST1

Perform these steps to start Node Manager on IDMHOST1:

1. Run the `startNodeManager.sh` script located under the `ORACLE_BASE/wlserver_10.3/server/bin` directory.
2. Run the `setNMProps.sh` script, which is located in the directory

```
ORACLE_BASE/product/fmw/oracle_common/common/bin
```

to set the `StartScriptEnabled` property to `true`:

```
IDMHOST1> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
IDMHOST1> ./setNMProps.sh
```

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

3. Stop the Node Manager by killing the Node Manager process.
4. Start Node Manager:

```
IDMHOST1> cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
IDMHOST1> ./startNodeManager.sh
```

6.5 Updating the Node Manager Credentials

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

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

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

```
IDMHOST1> cd ORACLE_BASE/admin/domain_name/aserver/domain_name/bin
HOST1> ./startWebLogic.sh
```

2. Use the Administration Console to update the Node Manager credentials.
 - a. In a browser, go to `http://ADMINVHN.mycompany.com:7001/console`.
 - b. Log in as the administrator.
 - c. Click **Lock and Edit**.
 - d. Click **Domain_name->Security->General** and expand **Advanced** at the bottom.
 - e. Enter a new username for Node Manager or make a note of the existing one and update the Node Manager password.
 - f. Save and activate the changes.
3. Stop the admin server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
4. Start WLST and connect to the node manager with `nmconnect` and the credentials set above. Then start the admin server using `nmstart`.

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

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

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

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

Note: `Admin_user` and `Admin_Password` are only used to authenticate connections between Node Manager and clients. They are independent from the server admin ID and password and are stored in the `ORACLE_BASE/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties` file.

5. Do not restart the Administration Server. It will be restarted in [Section 6.7, "Stopping and Starting the WebLogic Administration Server."](#)

6.6 Disabling Host Name Verification for the Oracle WebLogic Administration Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the administration server. (See [Chapter 16, "Setting Up Node Manager."](#)) If you have not configured the server certificates, you will receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the EDG topology configuration is complete as described in [Chapter 16, "Setting Up Node Manager."](#)

Perform these steps to disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock and Edit**.
3. Expand the Environment node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page appears.
5. Select **AdminServer(admin)** in the Names column of the table. The Settings page for AdminServer(admin) appears.
6. Click the **SSL** tab.
7. Click **Advanced**.
8. Set Hostname Verification to **None**.
9. Click **Save**.
10. Save and activate the changes.

6.7 Stopping and Starting the WebLogic Administration Server

1. Stop the administration server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#)
2. Start WLST and connect to the node manager with `nmconnect` and the credentials set previously described. Then start the administration server using `nmstart`.

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

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

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

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

Note: `Admin_user` and `Admin_Password` are only used to authenticate connections between Node Manager and clients. They are independent from the server admin ID and password and are stored in the `ORACLE_BASE/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties` file.

6.8 Validating the Administration Server

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

1. In a browser, go to `http://ADMINVHN.mycompany.com:7001/console`.
2. Log in as the WebLogic administrator, for example: `weblogic`.
3. Check that you can access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.
4. Log in to Oracle Enterprise Manager Fusion Middleware Control as the WebLogic administrator, for example: `weblogic`.

6.9 Configuring Oracle HTTP Server for the Administration Server

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

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

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

This file will have the following entries:

```
NameVirtualHost *:7777

<VirtualHost *:7777>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

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

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

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

</VirtualHost>
```

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

- Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

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

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

6.10 Registering Oracle HTTP Server With WebLogic Server

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

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

You must also run this command from WEBHOST2 for OHS2.

6.11 Setting the Front End URL for the Administration Console

Oracle WebLogic Server Administration Console tracks changes that are made to ports, channels and security using the console. When changes made through the console are activated, the console validates its current listen address, port and protocol. If the listen address, port and protocol are still valid, the console redirects the HTTP request, replacing the host and port information with the Administration Server's listen address and port. When the Administration Console is accessed using an load balancer, you must change the Administration Server's front end URL so that the user's browser is redirected to the appropriate load balancer address. To make this change, perform the following steps:

- Log in to Oracle WebLogic Server Administration Console.
- Click **Lock and Edit**.
- Expand the **Environment** node in the Domain Structure window.
- Click **Servers** to open the Summary of Servers page.
- Select **Admin Server** in the Names column of the table. The Settings page for AdminServer(admin) appears.
- Click the **Protocols** tab.
- Click the **HTTP** tab.
- Set the **Front End Host** field to `admin.mycompany.com` (your load balancer address).
- Set **FrontEnd HTTP Port** to 80
- Save and activate the changes.

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

6.12 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as `Running` in the Administration Console. If the server is shown as `Starting` or `Resuming`, wait for the server status to change to `Started`. If another status is reported (such as `Admin` or `Failed`), check the server output log files for errors. See [Section 18.6, "Troubleshooting"](#) for possible causes.

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

- <http://admin.mycompany.com/console>
- <http://admin.mycompany.com/em>

For information on configuring system access through the load balancer, see [Section 2.2.1, "Load Balancers."](#)

Note: After the registering Oracle HTTP Server as described in [Section 6.10, "Registering Oracle HTTP Server With WebLogic Server."](#)

the Oracle HTTP Server should appear as a manageable target in Enterprise Manager. To verify this, log into Oracle Enterprise Manager Fusion Middleware Control. The `WebTier` item in the navigation tree should show that Oracle HTTP Server has been registered.

6.13 Manually Failing Over the Administration Server

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

6.13.1 Failing over the Administration Server to IDMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from `IDMHOST1` to `IDMHOST2`.

Assumptions:

- The Administration Server is configured to listen on `ADMINVHN.mycompany.com`, and not on ANY address. See step 10 in [Section 6.2, "Running the Configuration Wizard on IDMHOST1 to Create a Domain."](#)
- The Administration Server is failed over from `IDMHOST1` to `IDMHOST2`, and the two nodes have these IP addresses:
 - `IDMHOST1: 100.200.140.165`
 - `IDMHOST2: 100.200.140.205`
 - `ADMINVIP: 100.200.140.206`

This is the Virtual IP address where the Administration Server is running, assigned to *interface:index* (for example, `eth1:2`), available in `IDMHOST1` and `IDMHOST2`.

- The domain directory where the administration server is running in `IDMHOST1` is on a shared storage and is mounted also from `IDMHOST2`.

Note: NM in IDMHOST2 does not control the domain at this point since `unpack/nmEnroll` has not been run yet on IDMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, node manager will be fully functional.

- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed in IDMHOST2 as described in previous chapters. That is, the same path for `ORACLE_HOME` and `MW_HOME` that exists in IDMHOST1 is available in IDMHOST2.

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

1. Stop the Administration Server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Migrate the IP address to the second node.
 - a. Run the following command as root on IDMHOST1 (where `x:y` is the current interface used by `ADMINVHN.mycompany.com`):

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

For example:

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

- b. Run the following command on IDMHOST2:

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

For example:

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

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

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

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

6.13.2 Starting the Administration Server on IDMHOST2

Perform the following steps to start Node Manager on IDMHOST2:

1. Run the `setNMProps.sh` script, which is located in the `ORACLE_BASE/product/fmw/oracle_common/common/bin` directory, to set the `StartScriptEnabled` property to `true` before starting Node Manager:

```
IDMHOST2> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
IDMHOST2> ./setNMProps.sh
```

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

2. Start Node Manager:

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

Start the Administration Server on IDMHOST2.

```
IDMHOST2> cd ORACLE_COMMON_HOME/common/bin
IDMHOST2> ./wlst.sh
```

Once in `wlst` shell, execute

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

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

- a. Ensure that you can access the Oracle WebLogic Server Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.
- b. Check that you can access and verify the status of components in the Oracle Enterprise Manager at `http://ADMINVHN.mycompany.com:7001/em`.

6.13.3 Validating Access to IDMHOST2 Through Oracle HTTP Server

Perform the same steps as in [Section 6.12, "Validating Access Through Oracle HTTP Server."](#) This is to check that you can access the Administration Server when it is running on IDMHOST2.

6.13.4 Failing the Administration Server Back to IDMHOST1

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

1. Make sure that the administration server is not running. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from `DOMAIN_HOME/bin`.
2. Run the following command on IDMHOST2.

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

3. Run the following command on IDMHOST1:

```
IDMHOST1> /sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
```

Note: Ensure that the netmask and interface to be used match the available network configuration in IDMHOST1

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

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

5. Start the Administration Server again on IDMHOST1.

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

Once in the wlst shell, execute

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

6. Test that you can access the Oracle WebLogic Server Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.
7. Check that you can access and verify the status of components in the Oracle Enterprise Manager at `http://ADMINVHN.mycompany.com:7001/em`.

6.14 Backing Up the Installation

After you have verified that the domain is working, back up the installation. This is a quick backup for the express purpose of immediate restore in case of problems in the further steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. At this point, you can initiate the regular deployment-specific backup and recovery process. The *Oracle Fusion Middleware Administrator's Guide* provides further details. For information on describing the Oracle HTTP Server data that must be backed up and restored, refer to the "Backup and Recovery Recommendations for Oracle HTTP Server" section in The *Oracle Fusion Middleware Administrator's Guide*. For information on how to recover components, see "Recovery of Components" and "Recovery After Loss of Component" sections in that guide. For recommendations specific to recovering from the loss of a host, see the "Recovering Oracle HTTP Server to a Different Host" in the guide. Also refer to the Oracle Database Backup and Recovery Guide for information on database backup.

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

1. Back up the web tier:
 - a. Shut down the instance as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
 - b. Back up the Middleware Home on the web tier using the following command (as root):


```
tar -cvpf BACKUP_LOCATION/web.tar MW_HOME
```
 - c. Back up the Instance home on the web tier using the following command, as root:


```
tar -cvpf BACKUP_LOCATION/web_instance.tar ORACLE_INSTANCE
```
 - d. Start the instance as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager. You can also use operating system tools such as `tar` for cold backups.
3. Back up the Administration Server domain directory to save your domain configuration. The configuration files all exist under the directory `ORACLE_BASE/admin/IDMDomain`

```
IDMHOST1> tar -cvpf edgdomainback.tar ORACLE_BASE/admin/IDMDomain
```

Extending the Domain with Oracle Internet Directory

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

This chapter includes the following topics:

[Section 7.1, "Prerequisites for Configuring Oracle Identity Directory Instances"](#)

[Section 7.2, "Configuring the Oracle Internet Directory Instances"](#)

[Section 7.3, "Post Configuration Steps"](#)

[Section 7.4, "Validating the Oracle Internet Directory Instances"](#)

[Section 7.5, "Backing up the OID Configuration"](#)

7.1 Prerequisites for Configuring Oracle Identity Directory Instances

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

1. Synchronize the time on Oracle Internet Directory, as described in [Section 7.1.1](#).
2. Install and upgrade the software on `OIDHOST1` and `OIDHOST2` as described in [Section 4.5.5](#) and [Section 4.6.1](#).
3. If you plan on provisioning the Oracle Internet Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on `OIDHOST1` and `OIDHOST2` as described in [Section 2.4](#).
4. Make sure that the load balancer is configured.

7.1.1 Synchronizing the Time on Oracle Internet Directory

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

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

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

7.2 Configuring the Oracle Internet Directory Instances

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

7.2.1 Configure the First Oracle Internet Directory Instance

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

On UNIX:

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

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

On UNIX:

Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
3. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports 389 and 636, as follows:

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

4. Start the Oracle Identity Management 11g Configuration Assistant by running `ORACLE_HOME/bin/config.sh`.
5. On the Welcome screen, click **Next**.
6. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
7. On the Specify Installation Location screen, specify the following values:
 - Oracle Instance Location: `/u01/app/oracle/admin/oid_inst1`
 - Oracle Instance Name: `oid_inst1`Click **Next**.
8. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.
 - Oracle Support Password: Provide the password for your My Oracle Support account.
 - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

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

Click **Next**.

11. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
 - **Connect String:**
`infradbhost1-vip.mycompany.com:1521:ldmdb1^infradbhost2-vip.mycompany.com:1521:ldmdb2@idmedg.mycompany.com`

Note: The Oracle RAC database connect string information must be provided in the format `host1:port1:instance1^host2:port2:instance2@servicename`. During this installation, it is not required for all the RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed. It is required that the information provided above is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances. Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.

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

Click **Next**.

12. On the Configure OID screen, specify the Realm and enter the Administrator (`cn=orcladmin`) password and click **Next**.
13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
14. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
16. To validate the installation of the Oracle Internet Directory instance on `OIDHOST1`, issue these commands:

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

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

7.2.2 Configuring an Additional Oracle Internet Directory Instance

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

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

On UNIX:

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

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

On UNIX:

Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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

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

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

On UNIX:

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

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

On UNIX, remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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

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

```
# The non-SSL port for Oracle Internet Directory
```

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

6. Start the Oracle Identity Management 11g Configuration Assistant by running `ORACLE_HOME/bin/config.sh`.
7. On the Welcome screen, click **Next**.
8. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
9. On the Specify Installation Location screen, specify the following values:
Oracle Instance Location: `/u01/app/oracle/admin/oid_inst1`
Oracle Instance Name: `oid_inst1`
Click **Next**.
10. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.
 - Oracle Support Password: Provide the password for your My Oracle Support account.
 - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.Click **Next**.
11. On the Configure Components screen, select Oracle Internet Directory, deselect all the other components, and click **Next**.
12. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.
Click **Next**.
13. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
 - Connect String:
`infradbhost1-vip.mycompany.com:1521:oidmdb1^infradbhost2-vip.mycompany.com:1521:oidmdb2@idmedg.mycompany.com`

Note: The Oracle RAC database connect string information needs to be provided in the format
host1:port1:instance1^host2:port2:instance2@service_name. During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.

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

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

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

Click **Next**.

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

Choose **Yes** to continue.

A popup window with this message appears:

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

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

Click **OK** to continue.

15. On the Specify OID Admin Password screen, specify the OID Admin password and click **Next**.
16. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
17. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
18. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
19. To validate the installation of the Oracle Internet Directory instance on OIDHOST2, issue these commands:

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

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

7.3 Post Configuration Steps

Follow the steps in this section to complete the configuration of the Oracle Internet Directory instances on `OIDHOST1` and `OIDHOST2`.

7.3.1 Registering Oracle Internet Directory with the Oracle WebLogic Server Domain

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

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

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

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

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

On `OIDHOST1`, issue this command:

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

On `OIDHOST2`, issue this command:

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

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

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

For example, on `OIDHOST1` and `OIDHOST2`:

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

The command requires login to WebLogic admin server (`idmhost1.mycompany.com`)

Username: `weblogic`

Password: `*****`

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

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

Syntax:

```
./emctl switchOMS <ReposURL>.
```

For Example:

```
./emctl switchOMS http://idmhost-vip.mycompany.com:7001/em/upload
```

Output:

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

5. Validate if the agents on OIDHOST1 and OIDHOST2 are configured properly to monitor their respective targets. Follow these steps to complete this task:
 - Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://idmhost1-vip.us.oracle.com:7001/em`.
Log in as the weblogic user.
 - From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**.
 - Validate that the hostname in Agent URL under the Agent column matches the hostname under the Host column. In case of a mismatch, follow the steps below to correct the issue:
 - Click the **configure** link to bring up the Configure Target Page.
 - On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.
 - Click **OK** to save your changes.

7.4 Validating the Oracle Internet Directory Instances

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

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

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

```

ldapbind -h oidhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oidhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oidhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oid.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oid.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1

```

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

7.5 Backing up the OID Configuration

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

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

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

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


```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Middleware home on the directory tier as the `root` user:


```
tar -cvpf BACKUP_LOCATION/dirtier.tar MW_HOME
```
 - c. Create a backup of the Instance home on the directory tier as the `root` user:


```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```
 - d. Start up the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:


```
ORACLE_INSTANCE/bin/opmnctl startall
```
2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. You can use an operating system tool such as `tar` for cold backups.
3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE/admin/domainName/aserver` directory:


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

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

For more information about backing up the directory tier configuration, see [Section 18.4, "Performing Backups and Recoveries."](#)

Extending the Domain with Oracle Virtual Directory

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

This chapter includes the following topics:

- [Section 8.1, "Prerequisites for Configuring Oracle Virtual Directory Instances"](#)
- [Section 8.2, "Configuring the Oracle Virtual Directory Instances"](#)
- [Section 8.3, "Post Configuration Steps"](#)
- [Section 8.4, "Validating the Oracle Virtual Directory Instances"](#)
- [Section 8.5, "Backing Up the Oracle Virtual Directory Configuration"](#)

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

8.1 Prerequisites for Configuring Oracle Virtual Directory Instances

Before configuring the Oracle Virtual Directory instances on OVDHOST1 and OVDHOST2, ensure that the following tasks have been performed:

8.1.1 Software, Network, and Directory Structure

8.2 Configuring the Oracle Virtual Directory Instances

1. Install and upgrade the software on OVDHOST1 and OVDHOST2 as described in the following sections:
 - [Section 4.5.5, "Installing the Oracle Identity and Access Management Suite"](#)
 - [Section 4.6.1, "Upgrading the Oracle Identity Management Platform and Directory Services Suite Oracle Home"](#)
2. If you plan on provisioning the Oracle Internet Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on OVDHOST1 and OVDHOST2 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

3. Make sure that the load balancer is configured as describe in [Section 2.2.2, "Configuring Virtual Server Names and Ports on the Load Balancer."](#)

8.2.1 Configuring the First Oracle Virtual Directory Instance

1. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

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

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

On UNIX:

Remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
3. Edit the `staticports.ini` file that you copied to the temporary directory to assign ports 6501 and 7501, as follows:

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

4. Start the Oracle Identity Management 11g Configuration Assistant by running `ORACLE_HOME/bin/config.sh`.
5. On the Welcome screen, click **Next**.
6. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
7. On the Specify Installation Location screen, specify the following values:
 - Oracle Instance Location: `/u01/app/oracle/admin/OVD_inst1`
 - Oracle Instance Name: `OVD_inst1`Click **Next**.
8. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.
 - Oracle Support Password: Provide the password for your My Oracle Support account.
 - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.Click **Next**.
9. On the Configure Components screen, select **Oracle Virtual Directory**, deselect all the other components, and then click **Next**.

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

Click **Next**.

11. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

- LDAP v3 Name Space: `dc=mycompany,dc=com`

In the OVD Administrator section, enter:

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

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

Click **Next**.

12. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
13. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
15. To validate the installation of the Oracle Virtual Directory instance on `OVDHOST1`, issue these commands:

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

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

8.2.2 Configuring an Additional Oracle Virtual Directory

The schema database must be running before you perform this task. Follow these steps to install Oracle Virtual Directory on `OVDHOST2`:

1. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

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

2. If the ports are in use (that is, if the command returns output identifying either port), you must free them.
3. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

On UNIX, remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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


```
# The non-SSL port for Oracle Virtual Directory
Oracle Virtual Directory port = 6501
# The SSL port for Oracle Virtual Directory
Oracle Virtual Directory (SSL) port = 7501
```
5. Start the Oracle Identity Management 11g Configuration Assistant by running `ORACLE_HOME/bin/config.sh`.
6. On the Welcome screen, click **Next**.
7. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
8. On the Specify Installation Location screen, specify the following values:
Oracle Instance Location: `/u01/app/oracle/admin/ovd_inst1`
Oracle Instance Name: `ovd_inst1`
Click **Next**.
9. On the Specify Email for Security Updates screen, specify these values:
 - **Email Address:** Provide the email address for your My Oracle Support account.
 - **Oracle Support Password:** Provide the password for your My Oracle Support account.
 - Check the checkbox next to the **I wish to receive security updates via My Oracle Support** field.
 Click **Next**.
10. On the Configure Components screen, select Oracle Virtual Directory, deselect all the other components, and click **Next**.
11. On the Configure Ports screen, select **Specify Ports Using Configuration File** and enter the full pathname to the `staticports.ini` file that you edited in the temporary directory.
Click **Next**.
12. On the Specify Virtual Directory screen: In the Client Listeners section, enter:
 - LDAP v3 Name Space: `dc=mycompany,dc=com`
 In the OVD Administrator section, enter:
 - Administrator User Name: `cn=orcladmin`
 - Password: `*****`
 - Confirm Password: `*****`
 Select **Configure the Administrative Server in secure mode**.
Click **Next**.

13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
14. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
16. To validate the installation of the Oracle Virtual Directory instance on OVDHOST2, issue these commands:

```
ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

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

8.3 Post Configuration Steps

After you finish configuring Oracle Virtual Directory, proceed as follows.

8.3.1 Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain

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

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

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

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

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

On OVDHOST1, issue this command:

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

On OVDHOST2, issue this command:

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

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

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

For example, on OVDHOST1 and OVDHOST2:

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

The command requires login to WebLogic admin server
(idmhost1.mycompany.com)

Username: weblogic

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

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

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

Syntax:

```
/emctl switchOMS <ReposURL>.
```

For Example:

```
/emctl switchOMS  
http://idmhost-vip.mycompany.com:7001/em/upload
```

Output:

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

5. Validate if the agents on `OIDHOST1` and `OIDHOST2` are configured properly to monitor their respective targets. Follow the steps below to complete this task:
 - Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://adminvhn.us.oracle.com:7001/em`. Log in as the `weblogic` user.
 - From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**
 - Validate that the hostname in Agent URL under the Agent column matches the hostname under the Host column. In case of a mismatch follow these steps to correct the issue:
 - Click **configure** to bring up the Configure Target Page.
 - On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.
 - Click **OK** to save your changes

8.3.2 Creating Server Certificates for the Oracle Virtual Directory Instances

Oracle Virtual Directory is configured to use the SSL Server Authentication Only Mode by default. When you use command line tools like `ldapbind` to validate a connection secured by the SSL Server Authentication Only mode, the server certificate must be

stored in an Oracle Wallet. Also, the wallet on each node should contain certificates from both OVDHOST1 and OVDHOST2.

Follow these steps to perform this task:

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

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

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

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

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

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

Note: The wallet on each node should contain certificates from both OVDHOST1 and OVDHOST2.

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

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

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

- For OVD_KEYSTORE_FILE, use:


```
ORACLE_INSTANCE/config/OVD/ovd1/keystores/keys.jks
```
 - For OVD_SERVER_CERT_ALIAS, use `serverselfsigned`.
 - For PASSWORD used for the `-storepass` option, use the `orcladmin` account password.
 - OVD_SERVER_CERT_FILE refers to the file where the certificate is saved. The `keytool` utility creates this file under the location and filename specified by the OVD_SERVER_CERT_FILE parameter.
-

8.3.3 Configuring Adapters in Oracle Virtual Directory

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

Oracle Virtual Directory Adapters can only be configured after Oracle Directory Services Manager is installed, as described in [Chapter 9, "Extending the Domain with Oracle Directory Integration Platform and ODSM."](#)

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

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

8.4 Validating the Oracle Virtual Directory Instances

To validate the OVD instances, ensure that you can connect to each Oracle Virtual Directory instance and the load balancing router using these `ldapbind` commands

Follow the steps in [Section 8.3.2, "Creating Server Certificates for the Oracle Virtual Directory Instances"](#) before running the `ldapbind` command with the SSL port.

```
ldapbind -h ovdhost1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q
ldapbind -h ovdhost2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h ovdhost2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q
ldapbind -h ovd.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h ovd.mycompany.com -p 636 -D "cn=orcladmin" -q -U 2 -W
"file://DIRECTORY_FOR_SSL_WALLET" -Q
```

8.5 Backing Up the Oracle Virtual Directory Configuration

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

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

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

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

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


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

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

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

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

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

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

- 2.** Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. You can use an operating system tool such as `tar` for cold backups.

- 3.** Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE/admin/domainName/aserver` directory:

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

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

For more information about backing up the directory tier configuration, see [Section 18.4, "Performing Backups and Recoveries."](#)

Extending the Domain with Oracle Directory Integration Platform and ODSM

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

Oracle Directory Integration Platform is an optional product. If it is not required in your environment, do not install it.

This chapter includes the following topics:

- [Section 9.1, "Extending the Oracle WebLogic Domain with Oracle Directory Integration Platform and ODSM"](#)
- [Section 9.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster"](#)
- [Section 9.3, "Provisioning the Managed Servers on the Local Disk"](#)
- [Section 9.4, "Validating the Application Tier Configuration"](#)
- [Section 9.5, "Creating the Oracle Internet Directory Adapter Using ODSM"](#)
- [Section 9.6, "Backing Up the Application Tier Configuration"](#)

9.1 Extending the Oracle WebLogic Domain with Oracle Directory Integration Platform and ODSM

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

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

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

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity*

Management manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Ensure that port 7006 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

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

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

On UNIX:

Remove the entries for port 7006 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

4. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
5. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
6. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

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

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

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

8. On the Welcome screen, click **Next**.
9. On the Select Domain screen, select **Extend Existing Domain** and enter the domain details:

- **Hostname:** ADMINVHN.mycompany.com
- **Port:** 7001
- **User Name:** weblogic
- **User Password:** <enter user password>

Click **Next**.

10. A dialog box with the following message appears:

```
The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer
```

to the Identity Management documentation for information on how to verify the domain is valid.

Click **OK** to continue.

This is a benign warning that you can ignore.

11. On the Specify Installation Location screen, specify the following values (the values for the Oracle Middleware Home Location and the Oracle Home Directory fields are prefilled. The values default to the Middleware home and Oracle home previously installed on IDMHOST1 in [Section 6.1, "Enabling ADMINVHN on IDMHOST1"](#)):

- **Oracle Middleware Home Location:** /u01/app/oracle/product/fmw
- **Oracle Home Directory:** idm
- **WebLogic Server Directory:**
/u01/app/oracle/product/fmw/wlserver_10.3
- **Oracle Instance Location:** /u01/app/oracle/admin/ods_inst1
- **Oracle Instance Name:** ods_inst1

Click **Next**.

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

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

Click **Next**.

13. On the Configure Components screen, select the following components:

- **Oracle Directory Integration Platform**
- **Management Components - Oracle Directory Services Manager**
-

Deselect all the other components.

Select the **Clustered** check box.

Click **Next**.

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

Click **Next**.

15. On the Specify OID Details screen, specify the following:

- **Hostname:** oid.mycompany.com
- **Port:** 636
- **Username:** cn=orcladmin
- **Password:** *****

Click **Next**.

16. On the Specify Schema Database screen, specify the following values:

- Connect String:

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

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

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

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

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

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

Click **Next**.

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

9.2 Expanding the Oracle Directory Integration Platform and ODSM Cluster

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

- [Section 9.2.1, "Installing and Configuring Oracle Directory Integration Platform and ODSM on IDMHOST2"](#)
- [Section 9.2.2, "Post-Installation Steps"](#)

9.2.1 Installing and Configuring Oracle Directory Integration Platform and ODSM on IDMHOST2

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

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity*

Management manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST2 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Ensure that port number 7006 is not in use by any service on the computer by issuing this command for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

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

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

On UNIX:

Remove the entries for port 7006 in the `/etc/services` file if the port is in use by a service and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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

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

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

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

7. On the Welcome screen, click **Next**.
8. On the Select Domain screen, select the **Expand Cluster** option and specify these values:
 - **Hostname:** ADMINVHN.mycompany.com
 - **Port:** 7001
 - **UserName:** weblogic
 - **User Password:** <Enter the password for the webLogic user>

Click **Next**.

9. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

Click **OK** to continue.

This is a benign warning that you can safely ignore.

10. On the Specify Installation Location screen, specify the following values. The values for the Oracle Middleware Home Location and the Oracle Home Directory fields are prefilled. The values default to the Middleware home and Oracle home previously installed on `IDMHOST1` in [Section 6.1, "Enabling ADMINVHN on IDMHOST1."](#)
 - **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`
 - **Oracle Home Directory:** `idm`
 - **WebLogic Server Directory:**
`/u01/app/oracle/product/fmw/wlserver_10.3`
 - **Oracle Instance Location:** `/u01/app/oracle/admin/ods_inst2`
 - **Oracle Instance Name:** `ods_inst2`

Click **Next**.

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

Click **Next**.

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

Click **Next**.

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

9.2.2 Post-Installation Steps

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

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

9.2.2.1 Copying the DIP Application from IDMHOST1 to IDMHOST2

Copy the Oracle Directory Integration Platform application from IDMHOST1 to IDMHOST2.

Copy the following directory on IDMHOST1:

```
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers/wls_ods1/applications
```

to the following location on IDMHOST2:

```
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers/wls_ods2/applications.
```

For example, from IDMHOST1, execute this command:

```
scp -rp \  
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers/wls_ods1/applications \  
user@IDMHOST2:/MW_HOME/user_\  
projects/domains/IDMDomain/config/fmwconfig/servers/wls_ods2/applications
```

9.2.2.2 Setting the Listen Address for the Managed Servers

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

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

9.2.2.3 Starting the Managed Server on IDMHOST2

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

1. In the left pane of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Clusters**.
2. Select the cluster (`cluster_ods`) containing the Managed Server (`wls_ods2`) you want to start.
3. Select **Control**.

4. Under **Managed Server Instances in this Cluster**, select the check box next to the Managed Server (`wls_ods2`) you want to start and click **Start**.
5. On the Server Life Cycle Assistant page, click **Yes** to confirm.

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

9.3 Provisioning the Managed Servers on the Local Disk

This section provides the steps to provision the Managed Server on the local disk. Proceed as follows:

1. Stop the Admin Server and the Managed Servers (`wls_ods1` and `wls_ods2`) as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Stop the Node Manager running on both `IDMHOST1` and `IDMHOST2` as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
3. On `IDMHOST1`, pack the Managed Server domain using the `pack` command located under the `ORACLE_HOME/common/bin` directory. Make sure to pass `managed=-true` flag to pack the managed server. Type:

```
ORACLE_HOME/common/bin/pack.sh -managed=true \  
-domain=path_to_adminServer_domain -template=templateName.jar \  
-template_name=templateName
```

For example

```
ORACLE_HOME/common/bin/pack.sh -managed=true \  
-domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain \  
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \  
-template_name=ManagedServer_Template
```

4. Unpack the Managed Server to the local disk on `IDMHOST1` using the `unpack` command located under the `ORACLE_COMMON_HOME/common/bin` directory.

```
ORACLE_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \  
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_HOME/common/bin/unpack.sh \  
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \  
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \  
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```

5. Copy the Managed Server template directory from `IDMHOST1` to `IDMHOST2`. For Example:

```
scp -rp /u01/app/oracle/products/fmw/templates  
user@IDMHOST2://u01/app/oracle/products/fmw/templates
```

6. Unpack the Managed Server to the local disk on `IDMHOST2` using the `unpack` command located under the `ORACLE_HOME/common/bin` directory.

```
ORACLE_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \  
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_HOME/common/bin/unpack.sh \
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applicationsStatus
```

7. Start the Node Manager on IDMHOST1 and IDMHOST2 using the `startNodeManager.sh` script located under the `WL_HOME/server/bin` directory. For Example:

```
/u01/app/oracle/product/fmw/wlserver_10.3/server/bin/startNodeManager.sh > \
/tmp/nm.log &
```

8. Start the Administration server from the shared disk on IDMHOST1 using the `startWebLogic.sh` script. For example:

```
/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/bin/startWebLogic.sh > \
/tmp/adminServer.out 2>&1 &
```

9. Validate that the Administration Server started up successfully by opening a browser accessing the Administration Console `http://ADMINVHN.us.oracle.com:7001/console`.

Also validate Enterprise Manager by opening a browser and accessing Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.us.oracle.com:7001/em`.

10. Start the Managed Servers on IDMHOST1 and IDMHOST2 by using the Administration Console by following the steps below
 - a. In the left pane of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Clusters**
 - b. Select the cluster (cluster_ods) containing the Managed Servers (wls_ods1, wls_ods2) you want to start.
 - c. Select **Control**.
 - d. Under Managed Server Instances in this Cluster, select the Managed Servers (wls_ods1, wls_ods2) and click **Start**.
 - e. On the Server Life Cycle Assistant page, click **Yes** to confirm.
11. Delete the `MW_HOME/user_projects` directory on IDMHOST1 and IDMHOST2. This directory is created by the Oracle Universal Installer when the domain is originally configured and is no longer required after the provisioning the Managed Server to the local disk.

9.4 Validating the Application Tier Configuration

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

9.4.1 Validating Oracle Directory Services Manager

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

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

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

For example, on IDMHOST1, enter this URL:

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

And on IDMHOST2, enter this URL:

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

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

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

- a. Launch Oracle Directory Services Manager from IDMHOST1:

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

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

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

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

- a. Launch Oracle Directory Services Manager from IDMHOST1:

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

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

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

9.4.2 Validating Oracle Directory Integration Platform

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

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

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

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

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

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

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

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

ODIP Application is active at this host and port.

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

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

ODIP Application is active at this host and port.

9.5 Creating the Oracle Internet Directory Adapter Using ODSM

Create an Oracle Virtual Directory adapter for Oracle Internet Directory using the following steps.

1. Log in to ODSM. You can get to ODSM either from Oracle Enterprise Manager Fusion Middleware Control or directly. To access ODSM from Fusion Middleware Control, go to `http://admin.mycompany.com:7001/em`, click **OVD**, then select **ODSM** from the **OVD** menu. To access ODSM directly, go to `http://admin.mycompany.com:7005/odsm`.
2. Create a connection to the Oracle Virtual Directory instance on OVDHOST1 and another connection to the instance on OVDHOST2, as follows:
 - a. Click **Create a New Connection**.
 - b. Supply the following information:
 - Directory Type:** OVD
 - Name:** myovd
 - Server:** Name of server OVD is running on, for example: OVDHOST1
 - Port:** Https port of the OVD. Determine this by typing:


```
opmnctl status -l
```
 - SSL Enabled:** Ensure this is selected
 - User Name:** cn=orcladmin
 - Password:** orcladmin password
 - c. Click **Connect**.
 - d. Accept the certificate when prompted.
3. Click the **Adapter** tab.
4. Click **Create Adapter**. The New Adapter Wizard appears.
5. On the Type Screen, supply the following information:
 - **Adapter Type:** LDAP.

- **Adapter Name:** OID Adapter.
 - **Adapter Template:** Oracle_Internet_Directory.
- Click Next.
6. On the DNS Setting Screen, for **Use DNS for Auto Discovery**, choose **No**.
Provide the following Connection Details
 - **Host:** oid.mycompany.com. port: 389
 - **Server Proxy Bind DN:** cn=orcladmin
 - **Proxy Password:** *orcladmin_password*Click Next.
 7. Ensure that the Connection Setting are successful.
Click Next.
 8. On the Name Space screen, provide the following information:
 - **Remote Base:** dc=mycompany, dc=com
 - **Mapped Namespace:** dc=mycompany, dc=comClick Next.
 9. Verify that the details provided on the Summary screen are accurate and click **Finish** to create the adapter.
 10. Repeat the Steps 3-9 on the second OVD host with exactly the same parameters and names.
 11. Stop and Start OVDHOST1 and OVDHOST2 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) so that the changes take effect.

9.6 Backing Up the Application Tier Configuration

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

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

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

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

```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Middleware Home on the application tier as the `root` user:

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

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

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

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

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

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

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

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

For information about backing up the application tier configuration, see [Section 18.4, "Performing Backups and Recoveries."](#)

Extending the Domain with Oracle Access Manager 10g

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

This chapter includes the following topics:

- [Section 10.1, "Introduction to Installing Oracle Access Manager"](#)
- [Section 10.2, "Prerequisites"](#)
- [Section 10.3, "Identity System Installation and Configuration"](#)
- [Section 10.4, "Access System Installation and Configuration"](#)
- [Section 10.5, "Backing Up the Oracle Access Manager Configuration"](#)

Note: After you complete the steps in this chapter, when you log in to the Administration Server console, it redirects you to the Oracle Access Manager Single Sign-on screen. Log in as an administrator such as `orcladmin`. Then the Oracle WebLogic Server login page appears. Log in as an Oracle WebLogic Server administrator.

10.1 Introduction to Installing Oracle Access Manager

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

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

chapter and [Chapter 19, "Configuring Single Sign-on for Administration Consoles"](#) to install and configure the Oracle Access Manager components necessary for your enterprise deployment.

For more information about Oracle Access Manager 10.1.4.3 and its various components, refer to the "Road Map to Manuals" section in the *Oracle Access Manager Introduction* manual, which includes a description of each manual in the Oracle Access Manager 10.1.4.3 documentation set.

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

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

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

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

10.1.2 Using Different LDAP Directory Stores

The Oracle Access Manager 11g enterprise deployment described in this manual ([Figure 1-2, "Oracle Access Manager 10g and Oracle Identity Manager 11g"](#)), shows Oracle Access Manager using Oracle Internet Directory as the only LDAP repository. Oracle Access Manager uses a single LDAP for policy and configuration data. It is possible to configure another LDAP as the identity store where users, organizations and groups reside. For example, an Oracle Access Manager instance may use Oracle Internet Directory as its policy and configuration store and point to an instance of Microsoft Active Directory for users and groups.

10.1.2.1 Using Oracle Virtual Directory as the Identity Store

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

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

10.2 Prerequisites

Before installing Oracle Access Manager components ensure that the following tasks have been performed:

1. Make `libgcc_s.so.1` and `libstdc++.so.5` available, as described in [Section 10.2.1](#).

2. Work around the installer bug, as described in [Section 10.2.2](#)

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

10.2.1 Making `libgcc_s.so.1` and `libstdc++.so.5` Available

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

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

Copy these libraries to a location accessible from the host where Oracle Access Manager is being installed. For example, use the home directory of the user installing Oracle Access Manager. In this case it is `/home/oracle`

10.2.2 Working Around the Installer Bug

There is a known bug with the Oracle Access Manager installer that sometimes manifests as a hang at install time on Linux. This is a third-party issue caused by InstallShield.

To work around this issue, follow these steps:

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

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

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

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

10.3 Identity System Installation and Configuration

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

10.3.1 Installing Identity Servers on OAMHOST1 and OAMHOST2

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

10.3.1.1 Installing the First Identity Server on OAMHOST1

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

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Identity Server" chapter of the *Oracle Access Manager Installation Guide*.
2. If you plan on provisioning the Oracle Access Manager Identity Server Components on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMHOST1 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Locate the Identity Server Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the installer's GUI console:

```
./Oracle_Access_Manager10_1_4_3_0_linux_Identity_Server -gui
```

4. On the Welcome to the InstallShield Wizard for Oracle Access Manager Identity Server screen, click **Next**.
5. Enter the username and group that the Identity Server will use. Specify `oracle/oinstall`.
Click **Next**.
6. Specify the installation directory for Oracle Access Manager Identity Server. Specify the following value:

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

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

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

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

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

Click **Next**.

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

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



8. Specify the location of the GCC run-time libraries, for example, `/home/oracle/oam_lib`.
Click **Next**.
9. On the Installation Progress screen, click **Next**.
10. On the first Identity Server Configuration screen, specify the transport security mode between the WebPass/Identity client and the Identity Server. The choices are:
 - **Open Mode:** No encryption.
 - **Simple Mode:** Encryption through SSL and a Public Key Certificate provided by Oracle.
 - **Cert Mode:** Encryption through SSL and a Public Key Certificate provided by an external CA.
 Choose **Open Mode**.
Click **Next**.
11. On the next Identity Server Configuration screen, specify the Identity Server ID, host name and port number for the Identity Server connection:
 - Enter a unique name for the Identity Server ID. For example: `IdentityServer_OAMHOST1`
 - Enter the hostname where the Identity Server will be installed. Make sure that the hostname can be resolved. For example: `oamhost1.mycompany.com`
 - Enter the port number on which this Identity Server communicates with its clients. For example, the default port number is 6022.
 Click **Next**.

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

Select **Yes**.

Click **Next**.

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

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

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

Do not select anything.

Click **Next**.

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

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

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

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

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

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

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

Click **Next**.

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

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

17. Specify your directory server configuration details:

- **Host machine or IP in which the directory server resides:**
 - oid.mycompany.com (if your user store is in Oracle Internet Directory)
 - ovd.mycompany.com (if your user store is in Oracle Virtual Directory)
- **Port Number:** 389 (non-SSL port)
- **Root DN:** cn=orcladmin (This is the default, unless you change the person object class during Identity System set up.)
- **Root Password:** The password for the user data directory server Root DN.

Click **Next**.

18. The Updating Directory schema to Directory Server screen appears. The update process can take some time.
19. Review the Readme file.

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

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

Click **Next**.

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

Note: If you want to use the NPTL threading model, run the `start_ois_server_nptl` script instead.

10.3.1.2 Installing the Second Identity Server on OAMHOST2

Follow these steps to install the second Oracle Access Manager Identity Server on OAMHOST2:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Identity Server" chapter of the *Oracle Access Manager Installation Guide*.
2. If you plan on provisioning the Oracle Access Manager Identity Server Components on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMHOST2 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Locate the Identity Server Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the Installer's GUI console:

```
./Oracle_Access_Manager10_1_4_3_0_linux_Identity_Server -gui
```

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

Click **Next**.

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

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

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

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

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

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

Click **Next**.

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

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



- Specify the location of the GCC run-time libraries, for example, `/home/oracle/oam_lib`.

Click **Next**.

- On the Installation Progress screen, click **Next**.
- On the first Identity Server Configuration screen, specify the transport security mode between the WebPass/Identity client and the Identity Server. The choices are:
 - Open Mode:** No encryption.
 - Simple Mode:** Encryption through SSL and a Public Key Certificate provided by Oracle.

- **Cert Mode:** Encryption through SSL and a Public Key Certificate provided by an external CA.

Choose **Open Mode**.

Click **Next**.

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

Click **Next**.

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

Select **No**.

Click **Next**.

13. On the next Identity Server Configuration screen, select the appropriate options if you want to set up SSL between the Identity Server and the Directory Server.
 - Directory Server hosting user data is in SSL
 - Directory Server hosting Oracle data is in SSL

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

Do not select anything.

Click **Next**.

14. This displays the configuration screen. After the configuration is completed, the ReadMe file displays.
15. Review the Readme file.

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

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

Click **Next**.

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

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

10.3.2 Installing Oracle HTTP Server on OAMADMINHOST

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

10.3.2.1 Installing Oracle HTTP Server

Follow these steps to install Oracle HTTP Server on OAMADMINHOST:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier* in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. If you plan on provisioning the Oracle HTTP Server on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMADMINHOST1, as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Oracle HTTP Server is installed on port 7777 by default. Ensure that ports 7777, 8889, and 4443 are not in use by any service on OAMADMINHOST by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

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

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

On UNIX:

Remove the entries for ports 7777, 8889, and 4443 in the `/etc/services` file if the ports are in use by a service and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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

```
#The http main port for ohs component  
OHS Port = 7777  
  
#This port indicates the OHS Proxy Port  
OHS Proxy Port = 8889  
  
#This port indicates the OHS SSL port  
OHS SSL Port = 4443
```

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

On UNIX, issue this command: `runInstaller`

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

The Specify Oracle Inventory screen is displayed.

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

Specify the Inventory Directory: /u01/app/oraInventory

Operating System Group Name: oinstall

A dialog box appears with the following message:

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

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

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

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

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

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

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

Click **Next**.

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

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

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

Click **Next**.

13. On the Specify WebLogic Domain screen, enter the location where you installed Oracle WebLogic Server. Note that the Administration Server must be running:

- **Domain Host Name:** idmhost-vip.us.oracle.com

- **Domain Port No:** 7001
- **User Name:** weblogic
- **Password:** *****

Click **Next**.

14. On the Specify Component Details screen, set the following values for OAMADMINHOST:

- **Instance Home Location:**
/u01/app/oracle/admin/oamAdmin_ohs
- **Instance Name:** oamAdmin_ohs
- **OHS Component Name:** oamAdmin_ohs

Click **Next**.

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

Click **Next**.

16. On the Email Address for Security Updates screen, specify these values:

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

Click **Next**.

17. On the Configuration Summary screen, ensure that the selections are correct and click **Install**.

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

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

20. Upgrade Oracle HTTP Server as described in [Section 4.4.3, "Upgrading Oracle HTTP Server from 11.1.1.2 to 11.1.1.3."](#)

10.3.2.2 Validating the Installation of Oracle HTTP Server

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

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

```
$ cd /u01/app/oracle/admin/oamAdmin_ohs/bin
$ ./opmnctl status
Processes in Instance: oamAdmin_ohs
```

ias-component	process-type	pid	status
oamAdmin_ohs	OHS	28575	Alive

2. Open a web browser and go to the URL `http://hostname.mycompany.com:port` to view the default Oracle HTTP Server Home page. For example:
`http://oamadminhost.mycompany.com:7777`

10.3.3 Installing WebPass on OAMADMINHOST

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

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing WebPass" chapter of the *Oracle Access Manager Installation Guide*.
2. If you plan on provisioning WebPass on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMADMINHOST1 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Locate the WebPass Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console:

```
./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebPass -gui
```

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

Click **Next**.

6. Specify the installation directory for Oracle Access Manager WebPass. For example, enter:

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

Click **Next**.

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

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

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

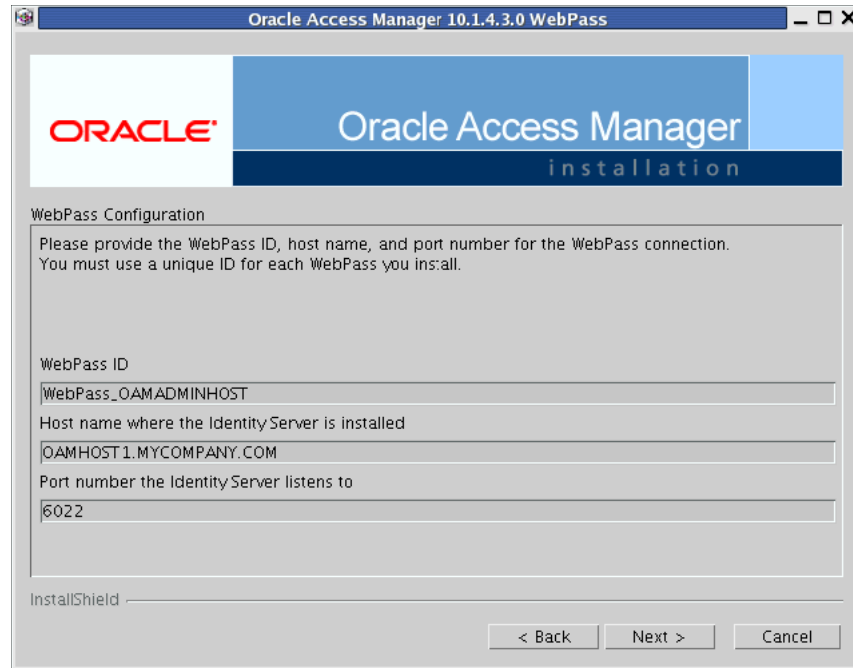
```
/u01/app/oracle/product/fmw/oam/webcomponents/identity
```

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

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



8. On the Oracle Access Manager WebPass Configuration screen, specify the location of the GCC run-time libraries. For example: `/home/oracle/oam_lib`
Click **Next**.
9. The Installing Oracle Access Manager WebPass screen appears.
10. When the WebPass Configuration screen appears, specify the Transport Security Protocol between the WebPass/Identity client and the Identity Server. Make sure to choose the same protocol as you did for the Identity Server. Select **Open Mode**.
Click **Next**.
11. The next screen in the WebPass Configuration series appears. Specify the WebPass ID, host name and port number for the Identity Server connection:
 - Enter a unique name for this WebPass ID. For example: `WebPass_OAMADMINHOST`
 - Enter the hostname of the Identity Server with which this WebPass should communicate. For example: `oamhost1.mycompany.com`
 - Enter the port number of the Identity Server with which this WebPass should communicate. For example, the default port number is 6022.Click **Next**.



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

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

Click **Next**.

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

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

For example:

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

Click **Next**.

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

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

Click **Next**.

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

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

16. A screen displays that advises you to launch a browser and open the *documentLocation* document for further information on configuring your web server.
Click **Next**.
17. On the Coreid 10.1.4.3.0 ReadMe screen, click **Next**.
18. The installation summary provides the details that you specified during this installation and instructs you to start the Identity Server at the conclusion of this installation. Click **Next**.
19. Click **Finish** to complete the installation.

10.3.3.1 Validating the WebPass Installation

Follow these steps to validate the WebPass installation:

1. Restart the Oracle HTTP server on OAMADMINHOST, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. To make sure that your Identity Server and WebPass Web server are running, navigate to the Identity System Console by specifying the following URL in your web browser:

```
http://hostname:port/identity/oblix
```

where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

3. The Identity System landing page should appear.
Do not select any link on the Identity System landing page because the system has not yet been set up.

10.3.4 Configuring Identity Servers Using WebPass

This section describes how to configure the Identity Servers on OAMHOST1 and OAMHOST2 using WebPass.

10.3.4.1 Configuring the First Identity Server

After the Identity Server and the WebPass instance are installed, you must specify the associations between them to make the system functional. Follow these steps to configure the first Identity Server:

1. Navigate to the Identity System Console by specifying the following URL in your web browser:

```
http://hostname:port/identity/oblix
```

where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

Click the **Identity System Console** link.

2. On the **System Console Application is not set up** page, click the **Setup** button.
3. On the **Product Setup page**, specify your user data directory server type. Select **Oracle Virtual Directory** or **Oracle Internet Directory** based on how your environment is configured.

Click **Next**.

4. On the **Schema Change** page, click **Next**. You do not need to do anything because the schema was updated during Identity Server installation.
5. Specify the user data directory details based on your installation:
 - **Host:** The DNS host name of the user data directory server. Enter:
oid.mycompany.com (if your user store is in Oracle Internet Directory)
ovd.mycompany.com (if your user store is in Oracle Virtual Directory)
 - **Port Number:** The port of the user data directory server. For example: 389
 - **Root DN:** The bind distinguished name of the user data directory server. For example: cn=orcladmin
 - **Root Password:** The password for the bind distinguished name.
 - **Directory Server Security Mode:** Open or SSL-enabled between the user data directory server and Identity Server. Select **Open**.
 - **Is Configuration data stored in this directory also?:** Yes (default)

Click **Next**.

ORACLE Product Setup

Location Of Directory Server with User Data

Enter the Host Name and Port Number of your Oracle Internet Directory.

If you don't have this information, go to the Oracle Directory Manager. The Port Number is displayed in the Login Dialog box. The Root DN is displayed under the System Passwords tab as Super User Name.

Enter server details here.

Host	<input type="text" value="oid.mycompany.com"/>
Port Number	<input type="text" value="389"/>
Root DN	<input type="text" value="cn=orcladmin"/>
Root Password	<input type="password" value="*****"/>
Directory Server Security Mode	<input checked="" type="radio"/> Open <input type="radio"/> SSL
Is the Configuration data stored in this directory also?	<input checked="" type="radio"/> Yes <input type="radio"/> No

6. On the **Location of Configuration Data and the Oracle Access Manager Searchbase** page, specify the distinguished name (DN) for the configuration data and the searchbase for user data. The configuration DN is the directory tree where Oracle Access Manager stores its configuration data. The searchbase is the node in the directory tree where the user data is stored and is usually the highest base for all user searches.

When the user data and configuration data are in the same directory, the entries can be specified as follows:

- **Configuration DN:** dc=mycompany, dc=com
- **Searchbase:** dc=mycompany, dc=com

Click **Next**.

Note: The configuration DN for the Oracle Access Manager Identity Server and the Oracle Access Manager Access Server must be the same. Also, if the configuration data and the search data are in different directories they should have unique DNs and the searchbase cannot be `o=Oblix, configurationDN` or `ou=Oblix, configurationDN`.

7. On the Person Object Class screen, specify the Person object class for the User Manager as shown below:

Person Object Class: *inetorgPerson*

Click the **Auto configure objectclass** text box.

Click **Next**.

Note: The person object class specified during this setup is the person object class used by the User Manager application.

8. On the Group Object Class screen, specify the Group object class as shown below. For example, the Group object class would be an entry resembling the following:

Group Object Class: *GroupofUniqueNames*

Click the **Auto configure objectclass** text box.

Click **Next**.

Note: The group object class specified during this setup is the only group object class used by the Group Manager application.

9. Stop the WebPass Web server instance on OAMADMINHOST by stopping the HTTP server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
10. Stop and then start the Identity Servers on OAMHOST1 and OAMHOST2 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
11. Start the WebPass Web server instance on OAMADMINHOST by starting the HTTP server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
12. On the Return to the Oracle Access Manager Product Setup window, click **Next**.
13. A screen appears summarizing the person object class changes that were made automatically with the following question: "Is the following configuration correct for the objectclass 'inetorgperson'?"
Review the Person object class attributes and then click **Yes**.
14. A screen appears summarizing the group object class changes that were made automatically with the following question: "Is the following configuration correct for the objectclass 'groupOfUniqueNames'?"
Review the Group object class attributes and then click **Yes**.

15. On the **Configure Administrators** page, the user `orcladmin` is configured as the Master Administrator by default. If you do not want to add any additional Administrator users, click **Next**.

ORACLE Product Setup

Configure Administrators

Select one or more persons to serve as the Oracle Access Manager Administrator, Master Identity Administrator, and Master Access Administrator. Oracle Access Manager Administrators have access to the System Configuration and System Management functions in both the Oracle Access Manager System and Access System. Master Identity Administrators have rights to the User Manager Configuration, Group Manager Configuration and Org. Manager Configuration applications in the Oracle Access Manager System. Master Access Administrators have rights to the Access System Configuration and System Management tabs in the Identity System Console. For more information, refer to the *Oracle Access Manager Administration Guide*.

Click the **Select User** button to choose administrators.

Master Admins: orcladmin **Select User**

Back **Next**

To add additional users as administrators, click the **Select User** button to bring up the Selector page.

ORACLE Identity Administration Selector

Search Full Name That Contains orcl All 8 Result Go Advanced

Done Cancel

Selector

Selected

Delete All Name

DEL orcladmin

Done Cancel

On the **Selector** page, complete the fields with the search criteria for the user you want to select as an administrator and click **Go**. A minimum of three characters is required to return search results.

ORACLE Identity Administration Selector

Search Full Name That Contains orcl All 8 Result Go Advanced

Done Cancel

Table View Custom View

Selected

Delete All Name

DEL orcladmin

Search Results

Previous Next

Add All Full Name*

ADD orcladmin

Previous Next

Done Cancel

16. Search results matching the specified criteria appear.
- Click **Add** next to the person you want to select as an administrator.
17. The name of the person appears under the **Selected** column on the right.
- Add other names as needed.
- Click **Done**.
18. On the **Configure Administrators** page, view the selected users listed as administrators.
- Click **Next**.
19. On the **Securing Data Directories** page, click **Done** to complete the Identity System setup.

20. Verify the configuration by performing these steps:

- a. Access the Oracle Access Manager system console at this URL:

`http://OAMADMINHOST:port/identity/oblix`

where *port* is the Oracle HTTP Server port.

For example, enter the following URL in your web browser:

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

- b. Click User Manager, Group Manager, or Org. Manager and log in with the newly created administrator user's credentials.

10.3.4.2 Configuring the Second Identity Server

Follow these steps to configure the second Identity Server:

1. Navigate to the Identity System Console by specifying the following URL in your web browser:

`http://hostname:port/identity/oblix`

where *hostname* refers to computer that hosts the WebPass Web server and *port* refers to the HTTP port number of the WebPass Web server instance.

For example, enter the following URL in your web browser:

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

Click the **Identity System Console** link.

2. A login dialog box appears.

Provide the administrator user name and password.

Click **Login**.

3. On the System Configuration screen, click the **Identity System Console** and select **System Configuration > Identity Servers**.

4. Click **Add** and specify the values shown below on the Add a new Identity Server screen:

- **Name:** idserver_oamhost2
- **Hostname:** oamhost2.mycompany.com
- **Port:** 6022
- **Debug:** Off
- **Debug File Name:** /oblix/logs/debugfile.lst
- **Transport Security:** Open

Accept the default values for the remaining parameters, unless required in your environment:

- **Maximum Session Time (hours):** 24 (default)
- **Number of Threads:** 20 (default)
- **Audit to Database Flag (auditing on/off):** Off (default)
- **Audit to File Flag (auditing on/off):** Off (default)
- **Audit File Name:** Leave blank (default)

- **Audit File Maximum Size (bytes):** 100000 (default)
- **Audit File Rotation Interval (seconds):** 7200 (default)
- **Audit Buffer Maximum Size (bytes):** 25000 (default)
- **Audit Buffer Flush Interval (seconds):** 7200 (default)
- **Scope File Name:** /oblix/logs/scopefile.lst (default)
- **SNMP State:** Off (default)
- **SNMP Agent Registration Port:** 80 (default)

ORACLE Identity Administration

System Configuration | User Manager Configuration | Group Manager Configuration | Org Manager Configuration | Common Configuration

Add a new Identity Server

Name	ldServer_OAMHOST2
Hostname	oamhost2.mycompany.com
Port	6022
Debug	<input checked="" type="radio"/> Off <input type="radio"/> On
Debug File Name	/oblix/logs/debugfile.lst
Transport Security	<input checked="" type="radio"/> Open <input type="radio"/> Simple <input type="radio"/> Cert
Maximum Session Time (hours)	24
Number of Threads	20
Audit to Database Flag (auditing on/off)	<input checked="" type="radio"/> Off <input type="radio"/> On
Audit to File Flag (auditing on/off)	<input checked="" type="radio"/> Off <input type="radio"/> On
Audit File Name	
Audit File Maximum Size (bytes)	100000
Audit File Rotation Interval (seconds)	7200
Audit Buffer Maximum Size (bytes)	25000
Audit Buffer Flush Interval (seconds)	7200
Scope File Name	/oblix/logs/scopefile.lst
SNMP State	<input checked="" type="radio"/> Off <input type="radio"/> On
SNMP Agent Registration Port	80

5. Click **Save**.
6. Click the Identity System Console and select **System Configuration > WebPass**.
7. The OAMWebPass_OAMADMINHOST instance is listed.
Click the WebPass instance for OAMADMINHOST.
8. On the Details for WebPass screen, click **List COREid Servers**.
9. The Identity Servers associated with the WebPass are listed.
Click **Add**.
10. On the Add a new Identity Server to the WebPass screen:
Select the identity server installed on OAMHOST2.
Select **Primary Server** and specify **2** connections.
Click **Add**.

11. On the List COREid Servers screen, select the identity server installed on OAMHOST1 and update the number of the connections to 2.

This completes the configuration of the Identity System.

You can now begin the installation of the Access System, which includes the Policy Manager, Access Server, and WebGate components.

10.4 Access System Installation and Configuration

This section provides details about the Access System installation and configuration. Access System components include the Policy Manager, Access Server, and WebGate components.

10.4.1 Installing the Policy Manager on OAMADMINHOST

The first step in installing the Access System is to install and configure the Policy Manager.

The Oracle Access Manager Policy Manager can be installed directly.

The Policy Manager must be installed in the same base directory as WebPass on OAMADMINHOST.

To install the Policy Manager, follow these steps:

1. Ensure that the system, patch, and other requirements are met. These are listed in the "Installing the Policy Manager" chapter of the *Oracle Access Manager Installation Guide*.
2. If you plan on provisioning Oracle Access Manager Policy Manager on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMADMINHOST1, as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Locate the Policy Manager Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console.

```
./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_PolicyManager -gui
```

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

Click **Next**.

6. You are prompted for the installation directory.

Specify the directory where you installed WebPass, for example:

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

Click **Next**.

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

The Policy Manager is installed in the `access` subdirectory created by the installer under the base location.

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

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

7. Oracle Access Manager Policy Manager will be installed in the following directory:

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



8. Specify the location of the GCC run-time libraries. For example, specify:
`/home/oracle/oam_lib`.

Click **Next**.

9. A progress message appears, then the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

Select **Oracle Internet Directory**.

10. You are prompted to specify whether policy data is in a separate directory server than the directory containing Oracle configuration data or user data, and if so, whether you would like the installer to automatically configure the directory server containing policy data.

Select **No**.

Click **Next**.

11. On the Configure Access Manager for using SSL mode with Directory Server screen, you are prompted for the communication method for Oracle Internet Directory.

These three options appear:

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

Do not select any of these options. Click **Next**.

12. On the Policy Manager Configure screen, you are asked to specify the transport security mode between this Access Manager and Access Servers that you plan to install in the future.

Choose **Open Mode**.

Click **Next**.

13. On the Configure Web Server screen, select **Yes** for the **Proceed with automatic updates of httpd.conf?** option.

Click **Next**.

14. Specify the full path of the directory containing the `httpd.conf` file. The path defaults to the `httpd.conf` file location for the Oracle HTTP Server installed on `OAMADMINHOST`.

Click **Next**.

A message informs you that the Web Server Configuration has been modified for Policy Manager.

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

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

Click **Next**.

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

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

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

Click **Next**.

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

19. A message appears informing you that the installation was successful.

Click **Finish**.

20. Stop and start the Oracle HTTP Server installed on OAMADMINHOST using the `opmnctl` commands shown below:

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

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

21. Stop and start the Identity Server installed on OAMHOST1 and OAMHOST2 using these commands:

```
ORACLE_HOME/identity/obltx/apps/common/bin/stop_ois_server
```

```
ORACLE_HOME/identity/obltx/apps/common/bin/start_ois_server
```

where *ORACLE_HOME* refers to the directory where the Identity Server is installed.

22. Validate that the Policy Manager installation was successful by opening a web browser and bringing up the Policy Manager Home page:

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

10.4.1.1 Configuring the Policy Manager

The Policy Manager must be configured to communicate with Oracle Internet Directory. Follow these steps to configure the communication:

1. Make sure your Web server is running.
2. Navigate to the Access System Console by specifying the following URL in your web browser:

```
http://hostname:port/access/obltx
```

where *hostname* refers to the host where the Policy Manager Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

Note: The WebPass and Policy Manager components share the same Oracle HTTP Server instance on OAMADMINHOST.

3. Click the **Access System Console** link.

A message informs you that the Administration Console Application is not yet set up.

4. Click the **Setup** button.

5. You are prompted for the User Directory Server Type.

If you are using Oracle Virtual Directory, choose **Data Anywhere** and if you are using Oracle Internet Directory, choose **Oracle Internet Directory**.

6. On the Location of Directory Server for User Data screen, specify the following server details:

- **Machine:** Specify the DNS host name of the user data directory server. Enter:

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

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

- **Port Number:** Specify the port of the user data directory server. Enter the non-SSL port for the directory server. For example: 389
- **Root DN:** Specify the bind DN (distinguished name) for the user data directory server. For example: cn=orcladmin
- **Root Password:** Specify the password for the bind distinguished name.
- **Directory Server Security Mode:** Select **Open**.

This screen capture shows the values for the Location of Directory Server for User Data screen if your user store is Oracle Internet Directory:

ORACLE Product Setup

Location Of Directory Server for User Data

Enter the Machine Name and Port Number of the Oracle Internet Directory that stores your *user data*.

If you don't know this information, use the Oracle Directory Manager. The Port # is displayed in the Login Dialog box. The Root DN is displayed under the System Passwords tab as Super User Name.

Note: Before reconfiguring an existing Access Manager, if you intend to modify any directory server details below, you must edit the profile for this directory server. Go to the Access System Console and select System Configuration > Configure Directory Options and edit the profile. Then run setup.

Enter server details here

Machine: oid.mycompany.com

Port Number: 389

Root DN: cn=orcladmin

Root Password: *****

Directory Server Security Mode: Open SSL

Back Next

This screen capture shows the values for the Location of Directory Server for User Data screen if your user store is Oracle Virtual Directory:

ORACLE Product Setup

Location Of Directory Server for User Data

Enter the Machine Name and Port Number of the Oracle Internet Directory that stores your *user data*.

If you don't know this information, use the Oracle Directory Manager. The Port # is displayed in the Login Dialog box. The Root DN is displayed under the System Passwords tab as Super User Name.

Note: Before reconfiguring an existing Access Manager, if you intend to modify any directory server details below, you must edit the profile for this directory server. Go to the Access System Console and select System Configuration > Configure Directory Options and edit the profile. Then run setup.

Enter server details here

Machine: ovd.mycompany.com

Port Number: 389

Root DN: cn=orcladmin

Root Password: *****

Directory Server Security Mode: Open SSL

Back Next

Click **Next**.

7. On the Directory Server Type containing Configuration Data screen, choose **Oracle Internet Directory**.

Click **Next**.

8. On the Directory Server containing User Data and Directory Server containing Configuration Data screen, a message informs you that the user data and configuration data can be stored in either the same or different directories.
Select **Store Configuration Data in the User Directory Server**.
Click **Next**.
9. On the Directory Server containing User Data and Directory Server containing Policy Data screen, a message informs you that the user data and policy data can be stored in either the same or different directories.
Select **Store Policy Data in the User Directory Server**.
10. On the Location of the Oracle Access Manager Configuration data, the Searchbase, and the Policybase screen, specify the appropriate information for your installation. For example:
 - **Searchbase:** `dc=mycompany, dc=com` (This must be the same searchbase you specified during Identity Server configuration)
 - **Configuration DN:** `dc=mycompany, dc=com` (This must be the same configuration DN you specified during Identity Server configuration)
 - **Policy Base:** `dc=mycompany, dc=com`Click **Next**.
11. On the Person Object Class screen, specify the Person object class that was specified during Identity Server system configuration:
Person Object Class: `inetorgperson`
Click **Next**.
12. You are prompted to restart the Web server. The Identity Servers must be restarted, along with the Web Server instance. Follow the sequence shown below:
 - a. Stop the Oracle HTTP Server on OAMADMINHOST as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
 - b. Restart the Identity Server on OAMHOST1 and OAMHOST2.
 - c. Start the Oracle HTTP Server on OAMADMINHOST as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)Click **Next**.
13. On the Root Directory for the Policy Domains screen, specify the root directory for policy domains.
Accept the default root directory for policy domains, for example:
Policy Domain Root: /
Click **Next**.
14. On the Configuring Authentication Schemes screen, select Yes to automatically configure authentication schemes.
Click **Next**.
15. On the next screen, select both **Basic Over LDAP** and **Client Certification authentication schemes**.
Click **Next**.

16. On the Define a new authentication scheme screen, specify the Basic over LDAP parameters. The values on the screen are prefilled. Review the parameters. Change the parameter values, if required by your environment:

- **Name:** Basic Over LDAP
- **Description:** This scheme is Basic over LDAP, using the built-in browser login mechanism
- **Level:** 1
- **Challenge Method:** Basic
- **Challenge Parameter:** realm: LDAP User Name/Password
- **Plugin(s):**

- **Plugin Name:** credential_mapping

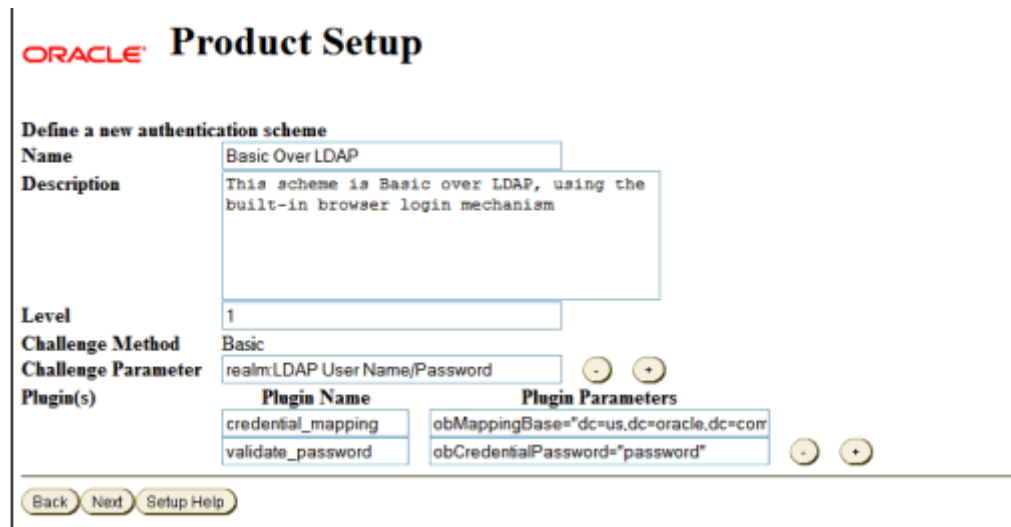
Plugin Parameters:

```
obMappingBase="dc=mycompany,dc=com",
obMappingFilter="(&(objectclass=inetorgperson)
(uid=%userid%))"
```

- **Plugin Name:** validate_password

Plugin Parameters: obCredentialPassword="password"

Click Next.



17. On the next Define a new authentication scheme screen, specify the Client Certificate parameters. The values on the screen are prefilled. Review the parameters. Change the parameter values, if required by your environment.

- **Name:** Client Certificate
- **Description:** This scheme uses SSL and X.509 client certificates
- **Level:** 2
- **Challenge Method:** Client Certificate
- **Challenge Parameter:** realm: LDAP User Name/Password

- **Plugin(s):**
 - **Plugin Name:** cert_decode
Plugin Parameters:
 - **Plugin Name:** credential_mapping
Plugin Parameters:

```
obMappingBase="dc=mycompany,dc=com",
obMappingFilter="(&(objectclass=inetorgperson)
(mail=%certSubject.E%))"
```

Click **Next**.

ORACLE **Product Setup**

Define a new authentication scheme

Name Client Certificate

Description This scheme uses SSL and X.509 client certificates

Level 2

Challenge Method Client Certificate

Plugin(s)

Plugin Name	Plugin Parameters
cert_decode	
credential_mapping	obMappingBase="dc=us.dc=oracle.dc=cor

Back Next Setup Help

18. On the Configure Policies to Protect NetPoint Identity System and Access Manager screen, select **Yes** to configure policies to protect Access System related URLs.
Click **Next**.
19. On the next page, instructions for Securing Data Directories and Configuring Identity and Access policy domains are shown. Review the instructions to complete the tasks and then restart the Identity Servers and web server instances by following the steps below:
 - a. Stop the WebPass/Policy Manager Web server instance on OAMADMINHOST.
 - b. Stop and then start the Identity Servers on OAMHOST1 and OAMHOST2. as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
 - c. Start the WebPass/Policy Manager Web server instance on OAMADMINHOST.

Verify that all the processes are back up again and then click **Done**.

20. The Policy Manager home page appears.
Confirm that the Policy Manager is installed correctly by performing the following steps:
 - a. Navigate to the Access System Console from your browser. For example:

`http://hostname:port/access/obliz`

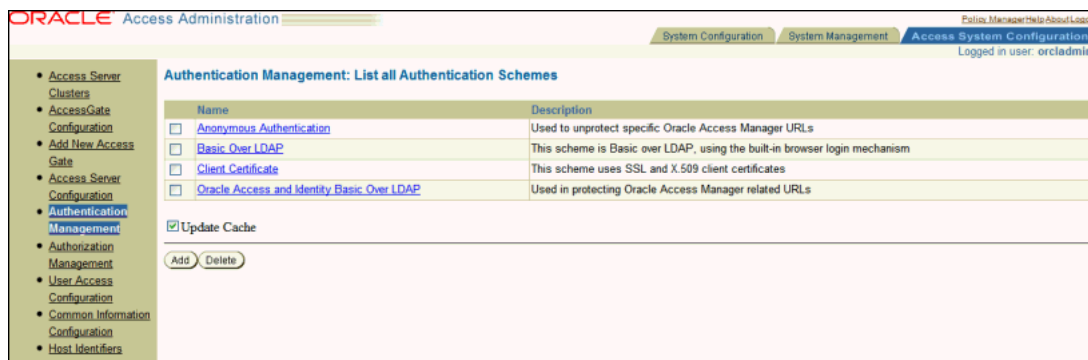
where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

- b. Select the **Access System Console** link.
- c. Log in as an administrator.
- d. Select the **Access System Configuration** tab, then click **Authentication Management** when it appears in the left column.

A list of the authentication schemes configured appears.



10.4.2 Installing the Access Server on OAMHOST1 and OAMHOST2

The second step in installing the Access System is to install the Access Server.

Before you begin installing the Access Server, you need to create an instance for it within the Access system Console.

10.4.2.1 Creating an Access Server Instance

Follow these steps to create an Access Server instance:

1. Log into the Access System Console by specifying the following URL in your web browser:

`http://hostname:port/access/obliz`

where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

2. On the Access System main page, click the **Access System Console** link, then log in as the administrator.
3. Click the **Access System Configuration** tab, then click **Access Server Configuration** when the side navigation bar appears.
4. Click **Add** to display the **Add Access Server** page with some defaults.

5. Specify the parameters shown below for the Access Server you plan to install:
- **Name:** Descriptive name for the Access Server that is different from any others already in use on this directory server. For example: `AccessServer_OAMHOST1`
 - **Hostname:** Name of the computer where the Access Server will be installed. The Access Server does not require a Web server instance. For example: `oamhost1.mycompany.com`
 - **Port:** Port on which the Access Server will listen. For example: `6023`
 - **Transport Security:** Transport security between all Access Servers and associated WebGates must match. Specify **Open**.
 - **Access Management Service:** This should be enabled only if the WebGate is using the Policy Manager API. In this case, select **ON**, since the WebGate will be using the PolicyManager API.

Review the remaining prefilled default values. Modify these values, if required by your environment.

Click **Save**.

ORACLE Access Administration

Add a new Access Server

Name	AccessServer_oamhost1
Hostname	oamhost1.mycompany.com
Port	6023
Debug	<input checked="" type="radio"/> Off <input type="radio"/> On
Debug File Name	
Transport Security	<input checked="" type="radio"/> Open <input type="radio"/> Simple <input type="radio"/> Cert
Maximum Client Session Time (hours)	24
Number of Threads	60
Access Management Service	<input type="radio"/> Off <input checked="" type="radio"/> On
Audit to Database (on/off)	<input checked="" type="radio"/> Off <input type="radio"/> On
Audit to File (on/off)	<input checked="" type="radio"/> Off <input type="radio"/> On
Audit File Name	
Audit File Size (bytes)	0
Buffer Size (bytes)	512000
File Rotation Interval (seconds)	0
Engine Configuration Refresh Period (seconds)	14400
URL Prefix Reload Period (seconds)	7200
Password Policy Reload Period (seconds)	7200
Maximum Elements in User Cache	100000
User Cache Timeout (seconds)	1800
Maximum Elements in Policy Cache	10000
Policy Cache Timeout (seconds)	7200
SNMP State	<input checked="" type="radio"/> Off <input type="radio"/> On
SNMP Agent Registration Port	
Session Token Cache	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Maximum Elements in Session Token Cache	10000

6. The **Access Server Configuration: List All Access Servers** page appears with a link to this instance. Verify that the Access Server has been created with the correct values by clicking on the link for the Access Server just created.
7. Repeat steps 3 through 6 for each additional Access Server you want to install. Substitute values where appropriate. For example, when creating the second Access Server instance, specify the following values:
 - **Name:** AccessServer_OAMHOST2
 - **Hostname:** oamhost2.mycompany.com
8. Click **Logout** and then close the browser window.

10.4.2.2 Starting the Access Server Installation

Follow these steps to start the Access Server installation:

1. Locate the AccessServer Installer on your Oracle Access Manager Software disk and start the installer as shown below. Pass the "-gui" option to bring up the GUI console. Log in as a user with Administrator privileges.

```
./Oracle_Access_Manager10_1_4_3_0_linux_Access_Server -gui
```

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

Click **Next**.

4. Specify the installation directory for Oracle Access Manager Access Server. For example, enter:

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

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

The Access Server is installed in the `access` subdirectory created by the installer under the base location.

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

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

Click **Next**.

5. Oracle Access Manager Access Server will be installed in the following location (the `access` directory is created by the installer automatically):

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




Click **Next**.

6. Specify the location of the GCC run-time libraries. For example:
/home/oracle/oam_lib.

Click **Next**.

The installation progress screen is shown. After the installation process completes, the Access Server Configuration screen appears.

7. On the Access Server Configuration screen, you are prompted for the transport security mode.

Specify the transport security mode. The transport security between all Access System components (Policy Manager, Access Servers, and associated WebGates) must match. Select one of the following: **Open Mode**, **Simple Mode**, or **Cert Mode**.

Select **Open Mode**.

Click **Next**.

8. On the next Access Server Configuration screen, you are prompted for the mode in which the Directory Server containing Oracle configuration data is running.

Select **Open**. This is the default choice.

On the same screen, specify the following directory server details:

- **Host:** Specify the DNS hostname of the Oracle configuration data directory server. For example: oid.mycompany.com
- **Port Number:** Specify the port of the Oracle configuration data directory server. For example: 389 (OID non-SSL Port)
- **Root DN:** Specify the bind distinguished name of the Oracle configuration data directory server. For example: cn=orcladmin
- **Root Password:** Specify the password for the bind distinguished name.

- **Type of the Directory Server containing Oracle configuration data:** Select **Oracle Internet Directory**.

Click **Next**.

9. On the next Access Server Configuration screen, specify where the Oracle Access Manager Policy data is stored. Select **Oracle Directory** and click **Next**.
10. On the next Access Server Configuration screen, specify the Access Server ID, the Configuration DN and the Policy Base specified when creating the Access Server instances in [Section 10.4.2.1, "Creating an Access Server Instance."](#)

Enter the requested details, for example:

- **Access Server ID:** AccessServer_OAMHOST1
- **Configuration DN:** dc=mycompany, dc=com
- **Policy Base:** dc=mycompany, dc=com



11. Review the information on the Oracle COREId 10.1.4.3 ReadMe screen.
Click **Next**.
12. A message appears informing you that the installation was successful.
Click **Finish**.
13. Start the Access Server so that you can confirm the Access Server is installed and operating properly.

To start the Access Server, follow these steps:

- a. Go to the following directory:

`ORACLE_HOME/access/oblix/apps/common/bin`

where `ORACLE_HOME` is the location where Oracle Access Manager Access Server is installed.

- b. Execute the following script:

```
start_access_server
```

If you want to use the NPTL threading model, execute the following script instead:

```
start_access_server_nptl
```

14. Repeat the preceding steps on OAMHOST2, substituting the hostname where appropriate.

10.4.3 Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2

The third step in installing the Access System is to install WebGate.

This section includes these topics:

10.4.3.1 About the Oracle Access Manager Configuration Tool

The Oracle Access Manager Configuration tool (OAM Configuration tool) is a command line utility provided to automatically enable single sign-on with Oracle Access Manager. The OAM Configuration tool runs a series of scripts and sets up the required policies. It requires a set of parameters as inputs. Specifically, the tool creates the following:

- A Form Authentication scheme in Oracle Access Manager
- Policies to enable authentication in the Oracle WebLogic Server
- Optionally, a WebGate profile in Oracle Access Manager to enable Oracle HTTP Server WebGates (from your web tier) to protect your configured applications. When this option is selected a WebGate profile is created for every application configured using the tool.
- A host identifier, depending on the scenario you choose. The host identifier is used to configure the WebGate hosts that send requests to your application. When a host identifier is not supplied, a default one is created with the "app_domain" name.
- Policies to protect and un-protect application-specific URLs. These policies would be configured for the host identifier created or provided in the previous step.

Note: If you plan on using an existing WebGate, the host identifier value of this WebGate must be used for the `web_domain` parameter when running the OAM Configuration tool.

10.4.3.2 Collecting the Information for the OAM Configuration Tool

Before you run the OAM Configuration tool, collect the following information:

- LDAP Host: The host name of the Directory Server or a load balancer address (in the case of a high availability or enterprise deployment configuration).
- LDAP Port: The port of the Directory Server.
- LDAP USER DN: The DN of the LDAP Administrator user. This will be a value such as `cn=orcladmin`.

- LDAP Password: Password of the LDAP Administrator user.
- oam_aaa_host: The host name of an Oracle Access Manager.
- oam_aaa_port: The port of an Oracle Access Manager.

10.4.3.3 Running the OAM Configuration Tool

Note: Currently, the OAM Configuration Tool fails when run in an environment where there are no Host Identifiers. As a temporary work around, follow these steps:

1. Log in to the Oracle Access Manager Console.
2. Click **Policy Manager**.
3. Select **Host Identifiers** on the left.
4. Create a dummy host identifier called `test`.
5. Delete this host identifier

Now run the OAM Configuration Tool.

Before you run the OAM Configuration tool, restart the following servers, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

- The Oracle HTTP server on OAMADMINHOST.
- The Access server on both OAMHOST1 and OAMHOST2.
- The Identity Server on both OAMHOST1 and OAMHOST2.

The OAM Configuration tool is located in the directory shown below. This tool can be run from any host that has Oracle Fusion Middleware 11g Release 1 installed.

`MW_HOME/oracle_common/modules/oracle.oamprovider_11.1.1/`

Set the JAVA_HOME value before running the tool as shown below:

```
export JAVA_HOME=$MW_HOME/jrockit_160_14_R27.6.4-18
```

The syntax for using the OAM Configuration tool is:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE [param=value]...
```

[Table 10–1](#) shows the basic OAM Configuration tool parameters and their values.

Table 10–1 Basic Parameters for the OAM Configuration Tool

Parameter	Value
app_domain	Oracle Access Manager policy domain name
web_domain	Name of the web domain. This is automatically created by the OAMCFGTOOL if no value is passed.
protected_uris	"uri1,uri2,uri3"
app_agent_password	Password to be provisioned for App Agent
ldap_host	Host name of LDAP server
ldap_port	Port of LDAP server
ldap_userdn	DN of LDAP Administrator user
ldap_userpassword	Password of LDAP Administrator user

Table 10–1 (Cont.) Basic Parameters for the OAM Configuration Tool

Parameter	Value
oam_aaa_host	Host name of an Oracle Access Manager
oam_aaa_port	Port of an Oracle Access Manager

The OAM Configuration tool has optional parameters that can be used for CREATE mode. [Table 10–2](#) shows those parameters.

Table 10–2 OAM Configuration Tool Optional Parameters for CREATE Mode

Parameter	Value
cookie_domain	Domain name to use for Single Sign-On cookie
public_uris	"uri1,uri2,uri3"
ldap_base	Base DN from which all LDAP searches will be done
oam_aaa_mode	One of OPEN, SIMPLE, CERT. Defaults to OPEN.
oam_aaa_passphrase	Passphrase required for SIMPLE mode
log_file	Name of the log file. Defaults to console output
log_level	One of ALL, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, OFF. Defaults to OFF.
output_ldif_file	Name of the LDIF file to store changes. If specified, will generate LDIF to be loaded later.

This is an example command for running the OAM Configuration tool when you want the tool to create a WebGate profile:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE app_domain="IDMEDG"
cookie_domain="mycompany.com"
protected_uris="/em,/console" app_agent_password="welcome1"
ldap_host=oid.us.oracle.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=password oam_aaa_host=oamhost1.mycompany.com
oam_aaa_port=6023
```

Notes:

1. The `web_domain` parameter should not be provided when you use the OAM Configuration Tool to create the WebGate profile.
 2. A Policy Domain must be created for each unique app domain in your environment.
 3. For this enterprise deployment topology use the OAM Configuration Tool to create one app domain called IDMEDG as shown in the previous example.
-
-

The following output is displayed when the command completes successfully:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
Operation Summary:
  Policy Domain : IDMEDG
  Host Identifier: IDMEDG
  Access Gate ID : IDMEDG_AG
```

Note: The Access Gate ID value above should be used as the WebGate ID when performing the WebGate installation described in [Section 10.4.3.7, "Installing the WebGate."](#)

This is an example command for running the OAM Configuration tool when you plan on using an existing WebGate:

```
$JAVA_HOME/bin/java -jar oamcfgtool.jar mode=CREATE app_domain="IDMEDG"
web_domain="idmEDG_WD" cookie_domain="mycompany.com"
protected_uris="/em,/console" app_agent_password="welcome1"
ldap_host=oid.us.oracle.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=<password> oam_aaa_host=oamhost1.mycompany.com
oam_aaa_port=6023
```

The following output is displayed when the command completes successfully:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
Operation Summary:
  Policy Domain : IDMEDG
  Host Identifier: idmedg_wd
  Access Gate ID : idmedg_wd_AG
```

To validate that the tool created the policies correctly, run the tool in **VALIDATE** mode:

```
java -jar oamcfgtool.jar mode=VALIDATE app_domain="IDMEDG"
ldap_host=oid.mycompany.com ldap_port=389 ldap_userdn="cn=orcladmin"
ldap_userpassword=welcome1 oam_aaa_host=oamhost1.mycompany.com oam_aaa_port=6023
test_username=orcladmin test_userpassword=welcome1
```

The output from the **VALIDATE** command is shown below:

```
Processed input parameters
Initialized Global Configuration
Validating app_domain: IDMEDG : OK.
Validating web_domain: IDMEDG : OK.
Validating access_gate: IDMEDG_AG : OK.
Found url:http://IDMEDG/public
Found url:http://IDMEDG/em
Found url:http://IDMEDG/console
Successfully completed the Validate operation
```

10.4.3.4 Updating the Host Identifier

The OAM Configuration Tool uses the value of the `app_domain` parameter to create a host identifier for the policy domain. This host identifier must be updated with all the hostnames variations for the host so that the configuration works correctly. Follow the steps below to update the host identifier created by the OAM Configuration Tool:

1. Navigate to the Access System Console by specifying the following URL in your web browser:

```
http://hostname:port/access/oblrix
```

where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

2. When prompted for a username and password, log in as an Administrator. Click **OK**.
3. On the Access System main page, click the **Access System Console** link.
4. On the Access System Console page, click the Access System Configuration tab.
5. On the Access System Configuration page, click **Host Identifiers** at the bottom left.
6. On the List all host identifiers page, click on the host identifier created by the OAM Configuration Tool. For example, select **IDMEDG**.
7. On the Host Identifier Details page, click **Modify**.
8. On the Modifying host identifier page, add all the possible hostname variations for the host. Click the plus and minus symbols to add or delete fields as necessary. The **Preferred HTTP Host** value used in the Access System Configuration must be added as one of the hostname variations. For example: `idmedg_wd`, `webhost1.mycompany.com:7777`, `admin.mycompany.com:7777`
9. Select the check box next to Update Cache and then click **Save**.
A message box with the following message is displayed: "Updating the cache at this point will flush all the caches in the system. Are you sure?"
Click **OK** to finish saving the configuration changes.
10. Verify the changes on the Host Identifier Details page.

10.4.3.5 Updating the WebGate Profile

The OAM Configuration Tool populates the `Preferred_HTTP_Host` and `hostname` attributes for the WebGate profile that is created with the value of the `app_domain` parameter. Both these attributes must be updated with the proper values for the configuration to work correctly. Follow the steps below to update the WebGate profile created by the OAM CFG Tool.

1. Navigate to the Access System Console by specifying the following URL in your web browser:

```
http://hostname:port/access/oblix
```

where *hostname* refers to the host where WebPass Oracle HTTP Server instance is running and *port* refers to the HTTP port of the Oracle HTTP Server instance.

For example, enter the following URL in your web browser:

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

2. On the Access System main page, click the **Access System Console** link, then log in as an Administrator.
3. On the Access System Console main page, click the **Access System Configuration** link to display the AccessGates Search page.
4. Enter the proper search criteria and click **Go** to display a list of AccessGates.

5. Select the AccessGate created by the OAM Configuration Tool. For example:
IDMEDG_AG
6. On the AccessGate Details page, select **Modify** to display the Modify AccessGate page.
7. On the Modify AccessGate page, update:
 - **Hostname:** Update the hostname with the name of the computer where WebGate is running. For example: `webhost1.mycompany.com`
 - **Preferred HTTP Host:** Update the Preferred_HTTP_Host with one of the hostname variations specified in the previous section, for example:
`admin.mycompany.com:7777`
 - **Primary HTTP Cookie Domain:** Update the Primary HTTP Cookie Domain with the Domain suffix of the host identifier, for example: `mycompany.com`.
 - **Maximum Connections:** Set to 4.
8. Click **Save**. A message box with the "Are you sure you want to commit these changes?" message is displayed.
9. Click **OK** to finish updating the configuration.
10. Verify the values displayed on the Details for AccessGate page to confirm that the updates were successful.

10.4.3.6 Assigning an Access Server to the WebGate

Follow these steps to assign an Access Server to the WebGate:

1. Log in as the Administrator.
2. Navigate to the **Details for AccessGate** page, if necessary. (From the **Access System Console**, select **Access System Configuration**, then **AccessGate Configuration**, then the link for the WebGate.)
3. On the **Details for AccessGate** page, click **List Access Servers**.
4. The Access Servers associated with the AccessGate are listed.
Click **Add**.
5. On the **Add a new Access Server to the Access Gate** screen, make the following selections:
 - Select the Access Server installed on OAMHOST2.
 - Select **Primary Server**, and specify **2** connections.Click the **Add** button to complete the association.
6. On the **List Access Servers** screen, select the Access server installed on OAMHOST1 and update the number of the connections to 2.
7. Repeat steps 3 through 6 to associate another Access Server to the WebGate.

10.4.3.7 Installing the WebGate

Follow these steps to install the WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2:

1. If you plan on provisioning WebGate on shared storage, ensure that the appropriate shared storage volumes are mounted on OAMADMINHOST1, WEBHOST1 and WEBHOST2 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

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

```
./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate -gui
```

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

Click **Next**.

5. Specify the installation directory for Oracle Access Manager Access Server. For example, enter:

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

Click **Next**.

Note: The base location for the Oracle Access Manager WebGate installation is `/u01/app/oracle/product/fmw/oam/webgate`. The WebGate component is installed in a subdirectory automatically created by the installer under this location.

The WebGate is installed in the `access` subdirectory created by the installer under the base location.

The `ORACLE_HOME` location for the Oracle Access Manager WebGate installation is:

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

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

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



7. Specify the location of the GCC run-time libraries, for example:
`/home/oracle/oam_lib.`
 Click **Next**.
8. The installation progress screen is shown. After the installation process completes, the WebGate Configuration screen appears.
9. On the WebGate Configuration screen you are prompted for the transport security mode.
 Specify the transport security mode. The transport security between all Access System components (Policy Manager, Access Servers, and associated WebGates) must match; select one of the following: **Open Mode**, **Simple Mode**, or **Cert Mode**.
 Select **Open Mode**.
 Click **Next**.
10. On the next WebGate Configuration screen, specify the following WebGate details:
 - **WebGate ID:** Specify the unique ID that identifies the WebGate profile in the Access System Console. Provide the Access Gate ID created by the OAM Configuration Tool in [Section 10.4.3.3, "Running the OAM Configuration Tool."](#)
 - **Password for WebGate:** Specify the password defined in the Access System Console.
 - **Access Server ID:** Specify the Access Server associated with the WebGate. For example: `AccessServer_OAMHOST1`
 - **DNS Hostname:** Specify the DNS host name where the Access Server associated with this WebGate is installed. For example:
`oamhost1.mycompany.com`

- **Port Number:** Specify the listen port for the Access Server.

Click **Next**.

11. On the Configure Web Server screen, click **Yes** to automatically update the web server, then click **Next**.
12. On the next Configure Web Server screen, specify the full path of the directory containing the `httpd.conf` file. The `httpd.conf` file is located under the following directory:

```
/u01/app/oracle/admin/ohsInstance/config/OHS/ohsComponentName
```

For example:

```
/u01/app/oracle/admin/ohs_instance2/config/OHS/ohs2/httpd.conf
```

Click **Next**.
13. On the next Configure Web Server page, a message informs you that the Web Server configuration has been modified for WebGate.
Click **Next**.
14. On the next Configure Web Server screen, the following message is displayed: "If the web server is setup in SSL mode, then `httpd.conf` file needs to be configured with the SSL related parameters. To manually tune your SSL configuration, please follow the instructions that come up".
Click **Next**.
15. On the next Configure Web Server screen, a message with the location of the document that has information on the rest of the product setup and Web Server configuration is displayed.

Select **No** and click **Next**.

16. The final Configure Web Server screen appears with a message to manually launch a browser and open the html document for further information on configuring your Web Server.

Click **Next**.

17. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next**.

18. A message appears (along with the details of the installation) informing you that the installation was successful.

Click **Finish**.

19. Restart your Web server, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

20. Verify the installation by performing the following steps:

- a. Ensure that the Identity Server, WebPass Web server, Policy Manager and Web Server, Access Server, and WebGate Web Server are running.

- b. Specify the following URL for WebGate diagnostics:

```
http://hostname:port/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

Where *hostname* refers to the host where the WebGate instance is running and *port* refers to HTTP port of the Oracle HTTP Server instance that is associated with the WebGate instance.

For example, use these URLs for the WebGate on each of the following hosts:

OAMADMINHOST:

```
http://oamadminhost.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

WEBHOST1:

```
http://webhost1.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

WEBHOST2:

```
http://webhost2.mycompany.com:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

The WebGate diagnostic page should appear. If the WebGate diagnostic page appears, the WebGate is functioning properly and you can dismiss the page.

10.5 Backing Up the Oracle Access Manager Configuration

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

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

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

1. Back up the Oracle Access Manager Identity Server.
 - a. Stop the Identity Server using the `stop_ois_server` script located under the `Identity_Server_ORACLE_HOME/oblix/apps/common/bin` directory.
 - b. Create a backup of the `Identity_Server_ORACLE_HOME` directory as the root user:


```
tar -cvpf BACKUP_LOCATION/IdentityServer.tar Identity_Server_ORACLE_HOME
```
 - c. Start the Identity Server using the `start_ois_server` script located under the `Identity_Server_ORACLE_HOME/oblix/apps/common/bin` directory.
2. Back up the Oracle Access Manager Access Server.
 - a. Stop the Access Server using the `stop_access_server` script located under the `Access_Server_ORACLE_HOME/oblix/apps/common/bin` directory.
 - b. Create a backup of the `Access_Server_ORACLE_HOME` directory as the root user:


```
tar -cvpf BACKUP_LOCATION/accessServer.tar Access_Server_ORACLE_HOME
```
 - c. Start the Access Server using the `start_access_server` script located under the `Access_Server_ORACLE_HOME/oblix/apps/common/bin` directory.
3. Back up the Oracle Access Manager WebPass, Policy Manager, Oracle HTTP Server, and WebGate.
 - a. Stop the Oracle Access Manager WebPass, Policy Manager, Webgate and Oracle HTTP Server instance. Stopping the Oracle HTTP Server instance using `opmnctl` to stop all four components, for example:


```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Oracle HTTP Server Middleware Home on the web tier as the root user:


```
tar -cvpf BACKUP_LOCATION/webtier.tar MW_HOME
```
 - c. Create a backup of the `INSTANCE_HOME` on the web tier as the root user:


```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```
 - d. Create a backup of the WebPass and Policy Manager `ORACLE_HOME`s as the root user:


```
tar -cvpf BACKUP_LOCATION/webPass.tar WEBPASS_ORACLE_HOME
tar -cvpf BACKUP_LOCATION/policyMgr.tar POLICY_MGR_ORACLE_HOME
```
 - e. Create a backup of the WebGate `ORACLE_HOME` as the root user:


```
tar -cvpf BACKUP_LOCATION/webGate.tar WEBGATE_ORACLE_HOME
```
 - f. Start up the instance using `opmnctl` under the `ORACLE_INSTANCE/bin` directory:


```
ORACLE_INSTANCE/bin/opmnctl startall
```
4. Back up the directory tier:

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

```
ORACLE_INSTANCE/bin/opmnctl stopall
```
- b. Create a backup of the Middleware Home on the directory tier as the root user:

```
tar -cvpf BACKUP_LOCATION/directorytier.tar MW_HOME
```
- c. Create a backup of the `INSTANCE_HOME` on the directory tier as the root user:

```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```
- d. Start up the instance using `opmnctl` under the `ORACLE_INSTANCE/bin` directory:

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

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

5. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager. An operating system tool such as `tar` can be used for cold backups.
6. Back up the Administration Server domain directory. This saves your domain configuration. All the configuration files exist under the `ORACLE_BASE/admin/domainName/aserver` directory:

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

For more information about backing up the Oracle Access Manager configuration, see [Section 18.4, "Performing Backups and Recoveries."](#)

Extending the Domain with Oracle Access Manager 11g

This chapter describes how to install and configure Oracle Access Manager 11.1.1 for use in the Oracle Identity Management enterprise deployment.

This chapter includes the following topics:

- [Section 11.1, "Introduction to Installing Oracle Access Manager"](#)
- [Section 11.2, "Prerequisites"](#)
- [Section 11.3, "Configuring Oracle Access Manager on IDMHOST1"](#)
- [Section 11.4, "Configure Oracle Access Manager on IDMHOST2"](#)
- [Section 11.5, "Configuring Oracle Access Manager to work with the Oracle Web Tier"](#)
- [Section 11.6, "Changing Request Cache Type"](#)
- [Section 11.7, "Configuring Oracle Access Manager to use an External LDAP store"](#)
- [Section 11.8, "Creating Policy Groups"](#)
- [Section 11.9, "Validating Oracle Access Manager"](#)

11.1 Introduction to Installing Oracle Access Manager

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

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

chapter and [Chapter 19, "Configuring Single Sign-on for Administration Consoles"](#) to install and configure the Oracle Access Manager components necessary for your enterprise deployment.

For more information about Oracle Access Manager 11.1.1 and its various components, refer to the "Road Map to Manuals" section in the *Oracle Access Manager Introduction* manual, which includes a description of each manual in the Oracle Access Manager 11.1.1 documentation set.

11.1.1 Using Different LDAP Directory Stores

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

11.1.2 Using Oracle Virtual Directory as the Identity Store

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

To learn more about the different types of directory configuration for Oracle Access Manager, consult the 11g Oracle Access Manager documentation at Oracle Technology Network. Customers considering these variations should adjust their directory tier and Oracle Access Manager deployment accordingly.

11.2 Prerequisites

Before you configure Oracle Access Manager, ensure that the following tasks have been performed on `IDMHOST1` and `IDMHOST2`:

1. Install Oracle WebLogic Server as described in [Section 4.5.3](#).
2. Install Oracle Identity and Access Management Suite as described in [Section 4.5.5](#).
3. Install Oracle Internet Directory as described in [Section 7.1](#) and [Section 7.2](#).
4. Install Oracle Virtual Directory as described in [Chapter 8](#).

11.3 Configuring Oracle Access Manager on IDMHOST1

Start the configuration wizard by executing the command:

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

Then proceed as follows:

1. On the Welcome screen, select **Extend an Existing WebLogic Domain**. Click **Next**.
2. On the Select a WebLogic Domain screen, using the navigator, select the domain home of the admin server, for example: `ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain`.
Click **Next**.
3. On the Select Extension Source screen, select **Oracle Access Manager with Database Policy Store**.

Click **Next**

4. The Configure RAC Multi Datasources screen shows the Multi Datasources if you have Oracle Directory Integration Platform or ODSM configured in your domain. Do not make any changes.

Click **Next**.

5. On the Configure JDBC Data Sources screen select the datasource **OAM Infrastructure**.

Select **Configure selected data sources as RAC multi data sources** in the next panel.

Click **Next**.

6. On the Configure RAC Multi Data Sources Screen:

- **Service Name:** Service name of the database that contains the OAM repository (`idmedg.mycompany.com`)
- **User Name:** EDG_OAM
- **Password:** Password for user EDG_OAM

In the top right box, click **Add** to add the second RAC node.

- **Host Name:** INFRADBHOST1
- **Instance Name:** idmdb1
- **Port:** 1521

Click **Add** again to add the second database host:

- **Host Name:** INFRADBHOST2
- **Instance Name:** idmdb2
- **Port:** 1521

Click **Next**.

7. On the Test Component Schema screen, the Wizard attempts to validate the data sources. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the problem, and try again.
8. On the Select Optional Configuration screen, select **Managed Servers, Clusters and Machines**.

Click **Next**

9. On the Configure Managed Servers screen, create one entry for each IDMHOST in the topology. To do this, click **Add** and supply the following information:
 - **Name:** WLS_OAM n where n is a sequential number.
 - **Listen Address:** The DNS name of the server that will host the managed server.
 - **Listen Port:** 14100

Note: When you first enter this screen the config wizard will have created a default managed server for you.

Change the details of the default managed server to reflect the details above. 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.

Leave all the other fields at the default settings. (If any Managed servers were defined during a previous installation, leave them as defined.)

Click **Next**.

10. On the Configure Clusters screen, create a cluster by clicking **Add**. Supply the following information:

- **Name:** `cluster_oam`
- **Cluster Messaging Mode:** `unicast`

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

11. On the Assign Servers to Clusters screen, associate the managed servers with the cluster. Click the cluster name in the right pane. Click the managed server under Servers, then click the arrow to assign it to the cluster.

The `cluster_oam` will have the managed servers `WLS_OAM1` and `WLS_OAM2`.

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

Click **Next**.

12. On the Configure Machines screen, create a machine for each host in the topology. Click on the tab **UNIX** if your hosts use Linux or a UNIX-based operating system. Otherwise, click on **machines**. Supply:

- **Name:** The name of the host. Best practice is to use the DNS name. For example: `idmhost1.mycompany.com` and `idmhost2.mycompany.com` for the first and second nodes respectively.
- **Node Manager Listen Address:** The DNS name of the machine. For example: `idmhost1.mycompany.com` and `idmhost2.mycompany.com` for the first and second nodes respectively.
- **Node Manager Port:** A port for node manager to use.

If you have already configured Oracle Directory Integration Platform or ODSM, machines will already exist for those hosts.

Click **Next**.

13. On the Assign Servers to Machines screen, indicate which managed servers will run on each of the machines you created.

Click a machine in the right pane.

Click the managed servers you want to run on that machine in the left pane.

Click the arrow to assign the managed servers to the machines. Repeat until all managed servers are assigned to machines. For example:

IDMHOST1: WLS_OAM1

IDMHOST2: WLS_OAM2

Click **Next** to continue.

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

Note: If you receive a warning that says:

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

Click **OK**.

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

15. Restart the Administration server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.3.1 Starting Oracle Access Manager Server on IDMHOST1

Start Oracle Access Manager on IDMHOST1 by following the start procedures in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) for:

- Admin Server (Restart if already running).
- Node Manager (if it is not already started)
- WebLogic Managed Server WLS_OAM1

11.3.2 Propagating the Domain Changes to the Managed Server Domain Directory

To propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory, proceed as follows:

1. Run the pack command on IDMHOST to create a template pack. Type the following commands:

```
IDMHOST1> cd MW_HOME/common/bin
IDMHOST1> ./pack.sh -managed=true -domain=ORACLE_
BASE/admin/IDMDomain/aserver/IDMDomain -template=idmdomaintemplate.jar
-template_name=IDMDomain_Template
```

2. Run the unpack command on IDMHOST1 to unpack the propagated template to the domain directory of the managed server. Type the following command:

```
IDMHOST1> ./unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain/
-template=idmdomaintemplate.jar -overwrite_domain=true -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

3. Restart managed server WLS_OAM1.

11.3.3 Remove IDM Domain Agent

To remove the IDM Domain Agent, do the following:

Log in to the WebLogic console using the URL:

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

Then:

1. Select **Security Realms** from the **Domain Structure** Menu
2. Click **myrealm**.
3. Click the **Providers** tab.
4. Click on **Lock and Edit** from the **Change Center**.
5. Select **IDMDomainAgent** from the list of authentication providers.
6. Click **Delete**.
7. Click **Yes** to confirm the deletion.
8. Click **Activate Changes** from the **Change Center**.
9. Restart the Administration server and ALL running managed servers, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.4 Configure Oracle Access Manager on IDMHOST2

Once the configuration has succeeded on IDMHOST1, you can propagate the configuration to IDMHOST2. You do this by packing the domain on IDMHOST1, using the pack script, and unpacking it on IDMHOST2 using the unpack script. Both scripts reside in `MW_HOME/oracle_common/common/bin`.

Type:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/  
-template=/tmp/IDMDomain.jar -template_name="OAM Domain" -managed=true
```

This creates a file called `IDMDomain.jar` in the `/tmp` directory. Copy this file to IDMHOST2.

Unpack the file on IDMHOST2 by using the unpack utility:

```
./unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain -template=MW_  
HOME/templates/IDMDomain.jar -overwrite_domain=true -app_dir=ORACLE_  
BASE/admin/IDMDomain/mserver/applications
```

11.4.1 Updating Node Manager Properties File on IDMHOST2

Before you start managed servers using the console, you must update the node manager property file to include `startScript=true`. You do this by running the script:

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

11.4.2 Starting Oracle Access Manager Server on IDMHOST2

Start Oracle Access Manager on IDMHOST2 by following the start procedures in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) for:

- Node Manager
- WebLogic Managed Server WLS_OAM1

11.5 Configuring Oracle Access Manager to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier

11.5.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on `WEBHOST1` and `WEBHOST2`.
2. Install and configure Oracle Access Manager on `IDMHOST1` and `IDMHOST2`.
3. Configure the loadbalancer with a virtual hostname (`sso.mycompany.com`) pointing to the web servers on `WEBHOST1` and `WEBHOST2`.
4. Configure the loadbalancer with a virtual hostname (`admin.mycompany.com`) pointing to web servers `WEBHOST1` and `WEBHOST2`.

11.5.2 Making Oracle Access Manager Server Aware of Load balancer

By default, Oracle Access Manager sends requests to the login page located on the local server. In an Enterprise deployment this needs to be changed so that login page requests are sent to the load balancer. Proceed as follows:

1. Log in to the OAM Console at:
`http://IDMHOST1.mycompany.com/oamconsole` as the `weblogic` user.
2. Click the **System Configuration** tab.
3. Double click **Server Instances**.
4. Click **SSO Engine** tab.
5. Enter the following information:
 - **OAM Server Host:** `sso.mycompany.com`
 - **OAM Server Port:** `443`
 - **OAM Server Protocol:** `https`
6. Click **Apply**.
7. Restart managed servers `WLS_OAM1` and `WLS_OAM2`, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.5.3 Configuring Oracle HTTP Servers to Display Login Page

On each of the web servers on `WEBHOST1` and `WEBHOST2` create a file called `oam.conf` in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`.

This file must contain the following information:

```
<Location /oam>
  SetHandler weblogic-handler
  WebLogicCluster idmhost1.mycompany.com:14100,idmhost2.mycompany.com:14100
</Location>
```

11.5.4 Configuring Oracle HTTP Servers to Access Oracle Access Manager Console

On each of the web servers on `WEBHOST1` and `WEBHOST2`, a file called `admin.conf` was created in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. (See [Section 6.9, "Configuring Oracle HTTP Server for the Administration Server"](#).) Edit this file and add the following lines within the virtual host definition:

```
<Location /oamconsole>
  SetHandler weblogic-handler
```

```

    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>
After editing the file should look like:

```

```

NameVirtualHost *:80

<VirtualHost *:80>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

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

<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

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

<Location /oamconsole>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>

</VirtualHost>

```

Restart the Oracle HTTP Server, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.5.5 Validating Accessibility

Attempt to access the OAM application using the URL:
<https://myso.mycompany.com:443/oam>

The Oracle Access Manager screen will be displayed. A message saying *Action Failed* will appear on the screen. You can ignore the message because all we are testing is that the OAM server can be accessed via the Load Balancer.

11.6 Changing Request Cache Type

In High Availability configurations, you must change the Request Cache type from BASIC to COOKIE. You change it by using `wlst`, as follows.

1. Set up the environment for `wlst` by running the command

```
DOMAIN_HOME/bin/setDomainEnv.sh
```

2. Start `wlst` by issuing the command:

```
ORACLE_HOME/common/bin/wlst.sh
```

3. Connect to your domain:

```
wls:/IDMDomain/serverConfig> connect()
```

Enter WebLogic Administration username and password.

Enter the URL for the WebLogic Administration Server in the format:

```
t3://IDMHOST1.mycompany.com:7001
```

4. Issue the command:

```
wls:/IDMDomain/serverConfig> configRequestCacheType(type="COOKIE")
```

5. Verify that the command has worked by issuing the command:

```
wls:/IDMDomain/serverConfig> displayRequestCacheType()
```

6. Exit WLS tool by issuing the command:

```
wls:/IDMDomain/serverConfig> exit()
```

7. Restart managed servers `WLS_OAM1` and `WLS_OAM2`, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.7 Configuring Oracle Access Manager to use an External LDAP store

By default, Oracle Access Manager uses its own built-in LDAP server. In the architecture we are building we use Oracle Virtual Directory (in front of Oracle Internet Directory) as our directory store. We modify Oracle Access Manager to use this directory store by using the Oracle Access Manager Console.

11.7.1 Creating Users and Groups in LDAP

Prior to performing this step, ensure that there is a group in your LDAP store for Oracle Access Manager administrators, such as `OAMAdministrator`, and that a user such as `oamadmin` exists in that group.

To do this create the following files:

oam_user.ldif

```
dn: cn=oamadmin,cn=Users,dc=mycompany,dc=com
cn: oamadmin
sn: oamadmin
description: oamadmin
uid: oamadmin
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
userpassword: mypasswd
```

oam_group.ldif

```
dn: cn=OAMAdministrator,cn=Groups,dc=mycompany,dc=com
cn: OAMAdministrator
displayname: OAMAdministrator
description: OAMAdministrator
uniquemember: cn=oamadmin,cn=Users,dc=mycompany,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup
```

Load the user and group into ldap using the following commands:

```
ldapadd -h myoid.mycompany.com -p 389 -D cn="orcladmin" -q -c -v -f oam_user.ldif
```

```
ldapadd -h myoid.mycompany.com -p 389 -D cn="orcladmin" -q -c -v -f oam_group.ldif
```

Note: These steps must be performed from the LDAP server.

11.7.2 Backing up Existing Configuration

Before starting the configuration backup the current configuration, so that should anything untoward happen the original configuration can be restored.

To achieve this, make a copy of the files `oam-config.xml` and `oam-policy.xml`. These files are located in the directory: `DOMAIN_HOME/config/fmwconfig`.

11.7.3 Creating User Identity Store

Go to the Oracle Access Manager console at the URL:

`http://adminvhn.mycompany.com:7001/oamconsole`

Log in using the WebLogic administration user.

Click **Add User Identity Store**.

- **Name:** LDAP_DIR
- **Ldap Provider:** OVD
- **LDAP URL:** `ldap://ovd.mycompany.com:389`
- **Principal:** `cn=orcladmin`
- **Credential:** `orcladmin password`
- **User Search Base:** `cn=Users,dc=mycompany,dc=com`
- **Group Search Base:** `cn=Groups,dc=mycompany,dc=com`
- **User Name Attribute:** `uid`
- **OAM Administrator's Role:** `OAMAdministrator`

Click **Apply**.

Click **Test Connection** to Validate the connection to the LDAP server.

11.7.4 Setting LDAP to Primary Authentication Store

Now that you have defined the LDAP identity store, you must set it as the primary authentication store. You do this by using the Oracle Access Manager console, as follows:

1. Click the **System Configuration** Tab
Select **Data Sources - User Identity Stores** from the navigation pane.
2. Click **LDAP_DIR**
Select **Open** from the **Actions** menu.
3. Click **Set as Primary**
4. Test the connection by clicking **Test Connection**
5. Restart the managed servers `Admin Server`, `WLS_OAM1` and `WLS_OAM2`, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.7.5 Validating the Configuration

Validate the configuration by logging in to the Oracle Access Manager console as the user `oamadmin`. You can access the console at:
`http://admin.mycompany.com/oamconsole`.

11.8 Creating Policy Groups

Out of the box the Identity Management Domain comes preconfigured with a number of default policies to protect such things as administration consoles. In addition it is recommended that Policy Groups be created to hold any policies which you may wish to create.

The policy groups you create are largely dependent on your environment and the way you wish to store your policy information. In this section of the guide, we will create two Policy Groups:

- Oracle Access Manager-Protected Resources: This policy group is used to hold details of resources that are protected by the OAM user/password policy.
- Oracle Adaptive Access Manager-Protected Resources: This policy group is used to hold details of resources that are protected using OAAM.

11.8.1 Creating Oracle Access Manager Policy Group

To create the OAM Policy Group perform the following steps:

Log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account created previously.

1. From the Navigation Window expand: **Application Domains > IDMDomainAgent**.
2. Click **Authentication Policies**
3. Click **Create** on the tool bar below the **Browse** tab).
4. Enter the following information:
 - **Name:** OAM Protected Resources
 - **Authentication Scheme:** LDAPScheme
5. Click **Apply**.

11.8.2 Creating Oracle Adaptive Access ManagerPolicy Group

1. From the Navigation Window expand: **Application Domains > IDMDomainAgent**.
2. Click **Authentication Policies**.
3. Click **Create** on the tool bar below the **Browse** tab).
4. Enter the following information:
 - **Name:** OAAM Protected Resources
 - **Authentication Scheme:** OAAMAdvanced
5. Click **Apply**.

11.9 Validating Oracle Access Manager

Validate Oracle Access Manager by protecting a simple resource.

For testing purposes it is good practice to create a simple HTML page, which you can use to test the functionality of OAM.

11.9.1 Creating a Test Resource

Create a test page called `sso.html` on `WEBHOST1` and `WEBHOST2`. The easiest way to do this is to create a file called `sso.html` in the directory `ORACLE_INSTANCE/config/OHS/component/htdocs` with the following content:

```
<html>
<body>
<center>
<p>
<h2>
SSO Protected Resource
</h2>
</p>
</center>
</body>
</html>
```

11.9.2 Creating a Resource

Now that you have something to protect, you need to create a resource in OAM and assign it to one of the policy groups you created above.

Log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account created previously.

1. From the Navigation window expand: **Application Domains > IDMDomainAgent**.
2. Click **Resources**.
3. Click **Create** on the tool bar below the **Browse** tab).
4. Enter the following information:
 - **Type:** http
 - **Host Identifier:** IDMDomain

- **Resource URL:** /sso.html
5. Click **Apply**.

11.9.3 Assigning Resource to Policy Group

Now that the resource exists, assign it to one of the policy groups you just created.

Log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account created previously.

1. From the Navigation window expand: **Application Domains > IDMDomainAgent > Authentication Policies**.
2. Click **OAM Protected Resources**.
3. Click **Edit** on the tool bar below the **Browse** tab.
4. In the Resources box, click **+**.
5. From the list, select the resource you created above.
6. Click **Apply**.

11.9.4 Adding Resource to Protected Resources

All that remains is to add the resource to the list of protected resources. To do this, log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account created previously.

1. From the Navigation window expand: **Application Domains > IDMDomainAgent > Authorization Policies**.
2. Click **Protected Resource Policy**.
3. Click **Edit** on the tool bar below the **Browse** tab.
4. In the Resources box, click **+**.
5. From the list, select the resource you just created.
6. Click **Apply**.

11.9.5 Validating Oracle Access Manager

To validate that Oracle Access Manager is working correctly:

Install Oracle Webgate as described in [Section 17.2, "Installing and Configuring WebGate"](#).

Access your protected resource using the URL:
`https://sso.mycompany.com:443/sso.html`.

The OAM Login page is displayed. Log in as an authorised OAM user, for example: `oamadmin`. Once you are logged in, the oam protected resource is displayed.

Extending the Domain with Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) is built on a J2EE-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 J2EE services available: a combination of Java, XML and object technologies. This architecture makes OAAM a scalable, fault-tolerant solution.

OAAM Apps is divided into following two components.

- OAAM Administration Applications
- OAAM Server Applications

This chapter describes the procedure to extend an existing IDM domain to include Oracle Adaptive Access Manager.

This chapter contains the following topics:

- [Section 12.1, "Prerequisites"](#)
- [Section 12.2, "Configuring Oracle Adaptive Access Manager on IDMHOST1"](#)
- [Section 12.3, "Start OAAMHOST1"](#)
- [Section 12.4, "Configuring Oracle Adaptive Access Manager on OAAMHOST2"](#)
- [Section 12.5, "Configuring Oracle Adaptive Access Manager to Work with the Oracle HTTP Server"](#)
- [Section 12.6, "Loading Oracle Adaptive Access Manager Seed Data"](#)

12.1 Prerequisites

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

1. Create a WebLogic domain described in [Chapter 6](#).
2. Install Oracle WebLogic Server, Oracle Fusion Middleware for Identity Management, and Oracle Identity and Access Management Suite as described in [Chapter 4](#).
3. Create a highly available database to hold the OAAM data. Pre-seed the database with OAAM data objects using the repository creation utility as described in [Section 3.3](#).
4. Install and configure Oracle Internet Directory as described in [Chapter 7](#).

5. Install and configure Oracle Virtual Directory as described in [Chapter 8](#).
6. Install Oracle HTTP Server on WEBHOST1 and WEBHOST2 as described in [Chapter 5](#).
7. Create Oracle Adaptive Access Manager Administrative groups and user in LDAP as described in [Section 12.1.1](#).
8. Create an Oracle Adaptive Access Manager Administration User in the WebLogic Console as described in [Section 12.2.3](#).

12.1.1 Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP

Before you extend the domain with OAAM, you must add a number of OAAM groups to the External LDAP store configured in [Chapter 7](#) and [Chapter 8](#). In addition to creating these groups, you must create a user and assign that user to these groups to facilitate access to the OAAM Admin console.

To do this, create the following files:

oaam_user.ldif

```
dn: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
cn: oaamadmin
sn: oaamadmin
description: oaamadmin
uid: oaamadmin
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
userpassword: mypasswd
```

oaam_group.ldif

```
dn: cn=OAAMCSRGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMCSRGroup
displayname: OAAMCSRGroup
description: OAAMCSRGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

dn: cn=OAAMCSRManagerGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMCSRManagerGroup
displayname: OAAMCSRManagerGroup
description: OAAMCSRManagerGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

dn: cn=OAAMEnvAdminGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMEnvAdminGroup
displayname: OAAMEnvAdminGroup
description: OAAMEnvAdminGroup
```

```

uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

```

```

dn: cn=OAAMInvestigationManagerGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMInvestigationManagerGroup
displayname: OAAMInvestigationManagerGroup
description: OAAMInvestigationManagerGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

```

```

dn: cn=OAAMInvestigatorGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMInvestigatorGroup
displayname: OAAMInvestigatorGroup
description: OAAMInvestigatorGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

```

```

dn: cn=OAAMRuleAdministratorGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMRuleAdministratorGroup
displayname: OAAMRuleAdministratorGroup
description: OAAMRuleAdministratorGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

```

```

dn: cn=OAAMSOAPServicesGroup,cn=Groups,dc=us,dc=oracle,dc=com
cn: OAAMSOAPServicesGroup
displayname: OAAMSOAPServicesGroup
description: OAAMSOAPServicesGroup
uniquemember: cn=oaamadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: top
objectclass: groupofuniquenames
objectclass: orclgroup

```

Load the user and group into LDAP issuing the following commands from the LDAP server:

```

ldapadd -h myoid.mycompany.com -p 389 -D cn="orcladmin" -w mypasswd -c -v \
-f oaam_user.ldif

```

```

ldapadd -h myoid.mycompany.com -p 389 -D cn="orcladmin" -w mypasswd -c -v \
-f oaam_group.ldif

```

12.2 Configuring Oracle Adaptive Access Manager on IDMHOST1

Although OAAM will be deployed on servers dedicated to it (OAAMHOST1 and OAAMHOST2), the Weblogic domain must first be extended with OAAM on IDMHOST1. Configure Oracle Adaptive Access manager on IDMHOST1 as follows.

12.2.1 Extending Domain for Oracle Adaptive Access Manager

Start the configuration wizard by executing the command:

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

Then proceed as follows:

1. On the Welcome Screen, select **Extend an Existing WebLogic Domain**. Click **Next**
2. On the Select a WebLogic Domain screen, using the navigator select the domain home of the admin server, for example: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain.

Click **Next**.

3. On the Select Extension Source screen, select the following:

- **Oracle Adaptive Access Manager - Server**
- **Oracle Adaptive Access Manager Admin Server**
- **Oracle WSM Policy Manager**
- **Oracle Identity Navigator**

Click **Next**

4. On the Configure RAC Multi Datasources screen (for ODSSM) click **Next**.
5. On the Configure JDBC Component Schema screen, select all of the data sources, then select **Configure selected data sources as RAC multi data sources**.

Click **Next**.

6. On the Configure RAC Multi Data Source Component Schema screen, select the first datasource (**OAAM Admin Schema**) and enter the following:

- **Data source:** OAAM Admin Server
- **Service Name:** oaam.mycompany.com
- **User Name:** EDG_OAAM
- **Password:** Password for above account.

7. In the top right box click **Add** to Add the first RAC node.

- **Host Name:** oaamdbhost1.mycompany.com
- **Instance Name:** oaamdb1
- **Port:** 1521

8. Click **Add** again to add the second RAC node.

- **Host Name:** oaamdbhost2.mycompany.com
- **Instance Name:** oaaamdb2
- **Port:**1521

9. Deselect this data source. Select the next data source, **OAAM Admin MDS Schema**, and enter the following information.

- **Data source:** OAAM Admin MDS Schema
- **Service Name:** oaam.mycompany.com
- **User Name:** EDG_MDS

- **Password:** Password for EDG_MDS account.
10. In the top right box click **Add** to add the first RAC node.
 - **Host Name:** oaamdbhost1.mycompany.com
 - **Instance Name:** oaamdb1
 - **Port:** 1521
 11. Click **Add** again to add the second RAC node.
 - **Host Name:** oaamdbhost2.mycompany.com
 - **Instance Name:** oaaamdb2
 - **Port:** 1521
 12. Deselect this data source. Select the next data source, **OAAM Server Schema**.
 - **Data source:** OAAM Server
 - **Service Name:** oaam.mycompany.com
 - **User Name:** EDG_OAAM
 - **Password:** Password for EDG_OAAM account.
 13. In the top right box click **Add** to add the second RAC node.
 - **Host Name:** oaamdbhost1.mycompany.com
 - **Instance Name:** oaamdb1
 - **Port:** 1521
 14. Click **Add** again to add the second RAC node.
 - **Host Name:** oaamdbhost2.mycompany.com
 - **Instance Name:** oaaamdb2
 - **Port:** 1521
 15. Deselect this data source. Select the next data source, **OWSM MDS Schema**.
 - **Data source:** OWSM MDS Schema
 - **Service Name:** idmdb.mycompany.com
 - **User Name:** EDG_MDS
 - **Password:** Password for EDG_MDS account.
 16. In the top right box click **Add** to add the second RAC node.
 - **Host Name:** infradbhost1.mycompany.com
 - **Instance Name:** idmdb1
 - **Port:** 1521
 17. Click **Add** again to add the second RAC Node.
 - **Host Name:** infradbhost2.mycompany.com
 - **Instance Name:** idmdb2
 - **Port:** 1521
 18. Deselect this data source. Click **Next**

19. 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.
20. On the Select Optional Configuration screen, select **Managed Server Clusters and Machines**. Click **Next**
21. When you first enter the Configure Managed Servers screen, the configuration wizard will have created a default managed server for you. *Change the details of the default managed server.*

Note: When you first enter this screen the config wizard will have created a default managed server 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.

For the **oaam_server** entry, *change the entry* to the following values:

- **Name:** WLS_OAAM1
- **Listen Address:** OAAMHOST1
- **Listen Port:**14300
- **SSL Listen Port:** 14301
- **SSL Enabled:** Selected.

For the second OAAM Server, click **Add** and supply the following information:

- **Name:** WLS_OAAM2
- **Listen Address:** OAAMHOST2
- **Listen Port:** 14300
- **SSL Listen Port:** 14301
- **SSL Enabled:** selected

Select the **OAAM_ADMIN_SERVER** entry.

Change the entry to the following values:

- **Name:** OAAMHOST1
- **Listen Address:** OAAMHOST2
- **Listen Port:**14200
- **SSL Listen Port:** 14201
- **SSL Enabled:** Selected

For the OAAM Admin Server, click **Add** and supply the following information:

- **Name:** WLS_OAAM_ADMIN2
- **Listen Address:** OAAMHOST2
- **Listen Port:** 14200
- **SSL Listen Port:** 14201

- **SSL Enabled** - selected
- Leave all the other fields at the default settings and click **Next**.
22. On the Configure Clusters screen, create a cluster by clicking **Add**.
- **Name:** cluster_oaam.
 - **Cluster Messaging Mode:** unicast
- Create a second cluster by clicking **Add**.
- **Name:** cluster_oaam_admin
 - **Cluster Messaging Mode:** unicast
- Leave all other fields at the default settings and click **Next**.
23. On the Assign Servers to Clusters screen, associate the managed servers with the cluster. Click the cluster name in the right pane. Click the managed server under **Servers**, then click the arrow to assign it to the cluster.

The cluster_oaam will have the managed servers **WLS_OAAM1** and **WLS_OAAM2**

The cluster_oaam_admin will have the managed servers **WLS_OAAM_ADMIN1** and **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**.

24. On the Configure Machines screen, create a machine for each host in the topology. Click the tab **UNIX** if your hosts use a UNIX-based operating system. Otherwise, click the **Machines** tab. Supply the following information:
- **Name:** Name of the host. Best practice is to use the DNS name (oaamhost1.mycompany.com).
 - **Node Manager Listen Address:** The DNS name of the machine (oaamhost1.mycompany.com)
 - **Node Manager Port:** A port for node manager to use

Click **Next**.

25. On the Assign Servers to Machines screen, indicate which managed servers will run on each of the machines you created.

Click a machine in the right pane.

Click the managed servers you want to run on that machine in the left pane.

Click the arrow to assign the managed servers to the machines.

Repeat until all managed servers are assigned to machines.

For example:

oaamhost1: wls_oaam1 and wls_oaam_admin1

oaamhost2:wls_oaam2 and wls_oaam_admin2

Click **Next** to continue.

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

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

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

click **OK**.

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

12.2.2 Starting Admin Server on IDMHOST1

Restart the Administration Server on IDM Host 1. See [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

12.2.3 Creating Oracle Adaptive Access Manager Administration User in WebLogic Console

Before you can access the OAAM administration console, you must create an administration user. Creating this user here allows you to use the OAAM administration console at this point. If you wire OAAM to OAM or you configure the Default Authenticator as described in chapter 19 then this user becomes redundant and if desired can be removed.

You create an administration user as follows:

1. Log in to Oracle WebLogic console at the URL:
`http://idmhost1.mycompany.com:7001/console` as the `weblogic` user.
2. From the domain structure menu, select **Security Realms**
3. Click **myrealm**.
4. Click the **Users and Groups** tab.
5. Click **New**.
6. Enter the following information:
 - **Name:** `oaadmin`
 - **Description:** OAAM Administrative user.
 - **Provider:** `DefaultAuthenticator`
 - **Password/Confirmation:** The password you want to assign to the user.
7. Click **OK**.
8. Click the newly created user **oaadmin**.
9. Click the **Groups** tab.
10. Assign all groups with the OAAM prefix to the user. Do this by selecting each group and clicking **>** to move it to the chosen group. The groups are:
 - **OAAMCSRGroup**
 - **OAAMCSRInvestigatorGroup**
 - **OAAMCSRManagerGroup**
 - **OAAMEnvAdminGroup**

- OAAMInvestigationManagerGroup
- OAAMRuleAdministratorGroup
- OAAMSOAPServicesGroup

11. Click Save.

12.2.4 Configuring Oracle Adaptive Access Manager on OAAMHOST1

Once the configuration has succeeded on IDMHOST1, you can propagate it to OAAMHOST1. You do this by packing the domain on IDMHOST1, using the pack script, and unpacking it on OAAMHOST1 using the unpack script. Both scripts reside in *MW_HOME/oracle_common/common/bin*.

On IDMHOST1, type:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
-template=/tmp/IDMDomain.jar -template_name="OAAM Domain" -managed=true
```

This creates a file called `IDMDomain.jar` in the `/tmp` directory. Copy this file to OAAMHOST1.

On OAAMHOST1, type:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain
-template=/tmp/IDMDomain.jar -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

12.3 Start OAAMHOST1

Start OAAMHOST1 from the console as follows.

12.3.1 Creating Node Manager Properties File on OAAMHOST1

Before you can start managed servers from the console, you must create a node manager property file. You do this by running the script `setNMProps.sh`, which is located in *MW_HOME/oracle_common/common/bin*. Type:

```
OAAMHOST1> $MW_HOME/oracle_common/common/bin/setNMProps.sh
```

12.3.2 Starting Oracle Adaptive Access Manager on OAAMHOST1

Start Oracle Access Manager on IDMHOST1 by following the start procedures in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) for:

- Node Manager
- WebLogic Managed Servers `WLS_OAAM1` and `WLS_OAAM_ADMIN1`

12.3.3 Validating OAAMHOST1

Validate the implementation by connecting to the OAAM Administration Server at `http://OAAMHOST1.mycompany.com:14200/oaam_admin`.

The implementation is valid if OAAM Admin console login page is displayed and you can login using the `oaamadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP"](#).

Validate the implementation by connecting to the OAAM Server at: `http://OAAMHOST1.mycompany.com:14300/oaam_server`.

The implementation is valid if the OAAM Server login page is displayed.

12.4 Configuring Oracle Adaptive Access Manager on OAAMHOST2

Configure Oracle Adaptive Access Manager on OAAMHOST2 as follows.

12.4.1 Deploying Domain on OAAMHOST2

Once the configuration has succeeded on IDMHOST1, you can propagate it to OAAMHOST2. You do this by packing the domain, using the `pack` script, on IDMHOST1 and unpacking it, using the `unpack` script on OAAMHOST2.

Both scripts reside in `MW_HOME/oracle_common/common/bin`.

On IDMHOST1, type:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/tmp/IDMDomain.jar -template_name="OAAM Domain" -managed=true
```

This creates a file called `IDMDomain.jar` in the `/tmp` directory. Copy this file to OAAMHOST2.

On OAAMHOST2, type:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain
-template=/tmp/IDMDomain.jar -template_name="OAAM Domain" -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

12.4.2 Starting OAAMHOST2

Start OAAMHOST2 from the console as follows.

12.4.2.1 Creating Node Manager Properties File on OAAMHOST2

Before you can start managed servers from the console, you must create a node manager property file. You do this by running the script `setNMProps.sh`, which is located in `MW_HOME/oracle_common/common/bin`. Type:

```
OAAMHOST2> $MW_HOME/oracle_common/common/bin/setNMProps.sh
```

12.4.2.2 Starting Oracle Adaptive Access Manager on OAAMHOST2

Start Oracle Adaptive Access Manager on OAAMHOST2 by following the start procedures in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) for:

- Admin Server
- Node Manager
- WebLogic Managed Servers `WLS_OAAM1` and `WLS_OAAM_ADMIN1`

12.4.3 Validating OAAMHOST2

Validate the implementation by connecting to the OAAM Administration Server at `http://OAAMHOST2.mycompany.com:14200/oaam_admin`. The implementation is valid if OAAM Admin console login page is displayed and you can login using the `oaadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP"](#).

Validate the implementation by connecting to the OAAM Server at:
`http://OAAMHOST2.mycompany.com:14300/oaam_server` The implementation
 is valid if the OAAM Server login page is displayed.

12.5 Configuring Oracle Adaptive Access Manager to Work with the Oracle HTTP Server

Configure Oracle Adaptive Access Manager to work with the Oracle HTTP Server, as follows.

12.5.1 Updating Oracle HTTP Server configuration

On each WEBHOST, create a file in `ORACLE_INSTANCE/config/OHS/ohs1/moduleconf` called `oaam.conf` with the following lines:

```
<Location /oaam_server>
  SetHandler weblogic-handler
  WebLogicCluster oaamhost1.mycompany.com:14300,oaamhost2.mycompany.com:14300
</Location>
```

The OAAM Admin console must only be available through the `admin.mycompany.com` site. You achieve this by editing the file `ORACLE_INSTANCE/config/OHS/component/moduleconf/admin.conf`. (You created `admin.conf` in [Section 6.9, "Configuring Oracle HTTP Server for the Administration Server"](#)).

Edit the virtual host definition in `admin.conf`.

After editing the file should look like this:

```
NameVirtualHost *:80

<VirtualHost *:80>

  ServerName admin.mycompany.com:80
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit

  # Admin Server and EM
  <Location /console>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
  </Location>

  <Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
  </Location>

  <Location /em>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
  </Location>
```

```
<Location /oaam_admin>
  SetHandler weblogic-handler
  WebLogicCluster oaamhost1.mycompany.com:14200,oaamhost2.mycompany.com:14200
</Location>
</VirtualHost>
```

12.5.2 Restarting Oracle HTTP Server

Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

12.5.3 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 into the WebLogic administration console at `http://admin.mycompany.com:7001/console`. Proceed as follows:

1. Select **Clusters** from the home page or, alternatively, select **Environment -> Clusters** from the Domain structure menu.
2. Click **Lock and Edit** in the Change Center Window to enable editing.
3. Click the Cluster Name (**cluster_oaam**).
4. In the General tab set WebLogic Plug in to **Enabled** by checking the box in the Advanced Properties section.
5. Click **Save**.
6. Select **HTTP** and enter the following values:
 - **Frontend Host:** `sso.mycompany.com`
 - **Frontend HTTP Port:** `80`
 - **Frontend HTTPS Port:** `443`

This ensures that any HTTPS URLs created from within WebLogic are directed to port 443 on the load balancer.

7. Click **Save**.
8. Select **Clusters** from the home page or, alternatively, select **Environment -> Clusters** from the Domain structure menu.
9. Click the Cluster Name (**cluster_oaam_admin**).
10. In the General tab, enable **WebLogic Plug in Enabled** by checking the box in the Advanced Properties section.
11. Click **Save**.
12. Select **HTTP** and enter the following values:
 - **Frontend Host:** `admin.mycompany.com`
 - **Frontend HTTP Port:** `80`
13. Click **Save**.
14. Click **Activate Changes** in the Change Center window to enable editing.

Restart Managed servers `WLS_OAAM1`, `WLS_OAAM2`, `WLS_OAAM_ADMIN1` and `WLS_OAAM_ADMIN2` as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

12.5.4 Validating Oracle Adaptive Access Manager

Log into the Oracle Adaptive Access Manager admin console, at `http://admin.mycompany.com/oaam_admin` using the `oaadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP"](#)

Also log into the Oracle Adaptive Access Manager server at `https://sso.mycompany.com/oam_server` in using the account `oaadmin` account and the password `test`.

Check that the following URL can be accessed:

`https://sso.mycompany.com:443/oam_server/oamLoginPage.jsp`

12.6 Loading Oracle Adaptive Access Manager Seed Data

Load seed data into Oracle Adaptive Access Manager as follows.

12.6.1 Loading Default Policies into OAAM Repository

Once OAAM has been installed, you must load default policies into the OAAM repository, as follows:

Log into the OAAM admin console at

`http://OAAMHOST2.mycompany.com:14200/oaam_admin` using the `oaadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP"](#).

Proceed as follows:

1. Double Click **Policies**.
2. Click **Import Policies**.
3. Click **Browse** and then select the file `ORACLE_HOME/oaam/init/oaam_sample_policies_for_uio_integration.zip`. Click **Open**.
4. Click **Import**.

12.6.2 Loading Knowledge Based Authentication Questions into Oracle Adaptive Access Manager Repository

Once OAAM has been installed, you must load default knowledge based authentication questions into the OAAM repository. Log into the OAAM admin console at `http://OAAMHOST2.mycompany.com:14200/oaam_admin` using the `oaam_admin` account you created. Proceed as follows:

1. Double click **KBA - Questions**.
2. Click **Import Questions**.
3. Click **Browse** and then select the file `IAM_ORACLE_HOME/oaam/kba_questions/oaam_kba_questions_en.zip`. Click **Click Browse** and then select the file `IAM_ORACLE_HOME/oaam/kba_questions/oaam_kba_questions_en.zip`. Click **Open**.

4. Click **Import**.

12.6.3 Loading Location data into Oracle Adaptive Access Manager Repository

Once you have installed Oracle Adaptive Access Manager at the default location, you must load data into the Oracle Adaptive Access Manager repository, as described in "Setting Up the CLI Environment" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

Extending the Domain with Oracle Identity Manager

This chapter describes how to install and configure Oracle Identity Manager 11.1.1 for use in the Oracle Identity Management Enterprise Deployment Topology.

This chapter contains the following topics:

- [Section 13.1, "Prerequisites"](#)
- [Section 13.2, "Extending the Domain to Configure Oracle Identity Manager and Oracle SOA Suite on IDMHOST1"](#)
- [Section 13.3, "Configuring Oracle Identity Manager on IDMHOST1"](#)
- [Section 13.4, "Propagating the Oracle Identity Manager and SOA Managed Servers to OIMHOST1 and OIMHOST2"](#)
- [Section 13.5, "Post-Installation Steps on OIMHOST1 and OIMHOST2"](#)
- [Section 13.6, "Post Installation Steps on OIMHOST2"](#)
- [Section 13.8, "Configuring Oracle Identity Manager to Work with the Oracle Web Tier"](#)
- [Section 13.9, "Configuring a Shared JMS Persistence Store"](#)
- [Section 13.10, "Configuring a Default Persistence Store for Transaction Recovery"](#)
- [Section 13.11, "Adding the CSF Entries for Oracle Identity Management and WSM"](#)

Oracle Identity Manager is a user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories. It also improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a stand-alone product or as part of Oracle Identity and Access Management Suite.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility through adapters.

Oracle Identity Manager provides the following key functionalities:

- User Administration
- Workflow and Policy
- Password Management

- Audit and Compliance Management
- Integration Solutions
- User Provisioning
- Organization and Role Management

For details about Oracle Identity Manager, see the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

13.1 Prerequisites

Before extending the domain with Oracle Identity Manager, ensure that the following tasks have been performed:

1. Install and upgrade the following software on `IDMHOST1`, `IDMHOST2`, `OIMHOST1` and `OIMHOST2`:
 - WebLogic Server: see [Section 4.5.3](#)
 - Oracle Identity and Access Management Suite: see [Section 4.5.5](#)
 - Oracle SOA Suite: see [Section 4.5.6](#)
2. Configure the Oracle Internet Directory instances, as described in [Section 7.1](#) and [Section 7.2](#).
3. Extend the domain with Oracle Virtual Directory as described in [Chapter 8](#).
4. Create the Oracle Internet Directory adapter using ODSM, as described in [Section 9.5](#).

Note: Oracle SOA deployed along with Oracle Identity Manager is used exclusively for Oracle Identity Manager work flow. It cannot be used for other purposes.

13.2 Extending the Domain to Configure Oracle Identity Manager and Oracle SOA Suite on `IDMHOST1`

Although OIM will be deployed on servers dedicated to it (`OIMHOST1` and `OIMHOST2`), the WebLogic domain must first be extended with OIM on `IDMHOST1`. Configure Oracle Identity Manager on `IDMHOST1` as follows.

To extend the domain on `IDMHOST1`, stop the WebLogic Administration Server and all the managed servers running in the domain. Then start the configuration wizard by executing the command:

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

Proceed as follows

1. On the Welcome screen, select **Extend an existing WebLogic Domain**.
Click **Next**.
2. On the Select WebLogic Domain Directory screen, select the location of the domain directory for the OIM domain. For Example:
`/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain`.
Click **Next**.

3. On the Select Extension Source screen, select **Extend my domain automatically to support the following added products**. From the list below, select: **Oracle Identity Manager**.

Note: Oracle SOA Suite and Oracle WSM Policy Manager are selected automatically.

Select **Next**.

4. The Configure RAC Multi Data Sources screen displays the schedulerDS Data Source configured for Oracle Directory Integration Platform and Oracle Directory Services manager (ODSM). Do not make any selections or changes on this screen.

Click **Next**.

5. On the Configure JDBC Component Schemas screen, select all the data sources listed on the page:

- SOA Infrastructure
- User Messaging Service
- OIM MDS Schema
- OWSM MDS Schema
- SOA MDS Schema
- OIM Schema

Select **Configure selected component schemas as RAC multi data source schemas** in the next panel.

Click **Next**.

6. On the Configure JDBC Data Source Component Schemas page, select all except the **OAM Infrastructure Multi Data Source Schemas** listed and then enter the following information:

Service Name: oimedg.us.oracle.com

For the First RAC Node:

- **HostName:** oimdb1.us.oracle.com
- **Instance Name:** oimedg1
- **Port:** 1521

For the second RAC Node (click **Add** to add an additional row):

- **HostName:** oimdb2.us.oracle.com
- **Instance Name:** oimedg2
- **Port:** 1521

Select each schema individually to enter the user name and password. For example:

Schema Name	Schema Owner	Password
SOA Infrastructure	EDG_SOAINFRA	<i>password</i>
User Messaging Service	EDG_ORASDPM	<i>password</i>

Schema Name	Schema Owner	Password
OIM MDS Schema	EDG_MDS	<i>password</i>
OWSM MDS Schema	EDG_MDS	<i>password</i>
SOA MDS Schema	EDG_MDS	<i>password</i>
OIM Infrastructure	EDG_OIM	<i>password</i>

Click **Next**.

Note: Do not select the OAM Infrastructure Multi Data Source Schema on this screen.

- On the Test Component Schema screen, the Configuration Wizard attempts to validate the data sources. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the problem, and try again.

Click **Next**.

- On the Select Optional Configuration screen, Select:
 - JMS Distributed Destination**
 - Managed Servers, Clusters and Machines**

Click **Next**.

- On the JMS Distributed Destination screen, make sure that all the JMS system resources listed on the screen are uniform distributed destinations. If they are not, select **UDD** form the drop down box. Make sure that the entries look like this:

JMS System Resource	Uniform/Weighted Distributed Destination
UMSJMSSystemResource	UDD
SOAJMSModule	UDD
OIMJMSModule	UDD

Click **Next**.

An Override Warning box with the following message is displayed:

CFGFWK-40915: At least one JMS system resource has been selected for conversion to a Uniform Distributed Destination (UDD). This conversion will take place only if the JMS System resource is assigned to a cluster

Click **OK** on the Override Warning box.

- When you first enter the Configure Managed Servers screen, the configuration wizard will have created a default managed server for you. Change the details of the default managed server. In addition, create a new entry by clicking **Add**. That is, there should be two entries for each OIMHOST in the topology.

For the Oracle Identity Management Managed Servers:

- Name:** WLS_OIM n where n is a sequential number
- Listen Address:** The DNS name of the server that will host the managed server

- **Listen Port:** 14000

For the SOA Managed Servers:

- **Name:** WLS_SOAn where *n* is a sequential number
- **Listen Address:** The DNS name of the server that will host the managed server
- **Listen Port:** 8001

Click **Next**.

Note: Do not change the configuration of any managed servers that have already been configured as part of previous application deployments.

11. On the Configure Clusters screen, create two clusters, by clicking **Add**. Supply the following information:

OIM Cluster:

- **Name:** cluster_oim
- **Cluster Messaging Mode:** unicast

SOA Cluster:

- **Name:** cluster_soa
- **Cluster Messaging Mode:** unicast

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

Note: Do not make any changes to the cluster_oam and the cluster_soa entries.

12. On the Assign Servers to Clusters screen, associate the managed servers with the cluster. Click the cluster name in the right pane. Click the managed server under **Servers**, then click the arrow to assign it to the cluster.

The **cluster_oim** will have the managed servers **WLS_OIM1** and **WLS_OIM2** as members.

The **cluster_soa** will have the managed servers **WLS_SOA1** and **WLS_SOA2** as members.

Click **Next**.

Note: Do not make any changes to the cluster_oam and the cluster_soa entries.

13. On the Configure Machines screen, create a machine for each host in the topology. Click the tab **UNIX** if your hosts use Linux or a UNIX-based operating system. Otherwise, click **Machines**. Supply the following information:

- **Name:** Name of the host. Best practice is to use the DNS name. For example: oimhost1.mycompany.com and oimhost2.mycompany.com for the first and second nodes respectively.

- **Node Manager Listen Address:** DNS name of the machine. For example: `oimhost1.mycompany.com` and `oimhost2.mycompany.com` for the first and second nodes respectively.
- **Node Manager Port:** Port for Node Manager

Click **Next**.

14. On the Assign Servers to Machines screen, indicate which managed servers will run on each of the machines you created.

Click a machine in the right pane.

Click the managed servers you want to run on that machine in the left pane.

Click the arrow to assign the managed servers to the machines.

Repeat until all managed servers are assigned to machines.

For example:

- **OIMHOST1:** `WLS_OIM1` and `WLS_SOA1`
- **OIMHOST2:** `WLS_OIM2` and `WLS_SOA2`

Click **Next** to continue.

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

13.3 Configuring Oracle Identity Manager on IDMHOST1

After you have extended the domain, configure the Oracle Identity Manager and SOA Managed Servers before starting them.

13.3.1 Prerequisites for Configuring Oracle Identity Manager

Before configuring Oracle Identity Manager, ensure that the following tasks have been performed:

1. Configure Oracle Internet Directory using the LDAP configuration pre-setup script, as described in [Section 13.3.1.1](#).
2. Create the Adapters in Oracle Virtual Directory, as described in [Section 13.3.1.2](#)

13.3.1.1 Configuring Oracle Internet Directory using the LDAP Configuration Pre-setup Script

The Oracle Identity Manager LDAP configuration pre-setup script adds the users, group and schemas required by OIM in OID. The LDAP configuration pre-setup script is located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory. To run the script, follow these steps:

1. Edit the `ldapconfig.props` file located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory and provide the following values:

Parameter	Value
OIMProviderURL	t3://oimhost1.us.oracle.com:14000, t3://oimhost2.us.oracle.com:14000
OIDURL	oid.mycompany.com

Parameter	Value
OIDAdminUsername	cn=orcladmin
OIDSearchBase	dc=mycompany,dc=com
UserContainerName	cn=OIMUsers
RoleContainerName	cn=OIMRoles
ReservationContainerName	ReservationContainerName

Note:

- The OIMProviderURL is not used by the LDAP configuration pre-setup script. It is only used by the LDAP configuration post-setup script.
- The OIDURL above refers to the OID URL. Do not substitute the OVD URL.

2. Save the file.**3.** Set the JAVA_HOME and the WL_HOME.

```
JAVA_HOME=ORACLE_BASE/product/fmw//jdk160_18
WL_HOME=ORACLE_BASE/product/fmw/wlserver_10.3
```

Note: The JAVA_HOME must be set to the SUN JDK.

4. Run LDAPConfigPreSetup.sh. The script prompts for the Oracle Internet Directory administrator password and the Oracle Identity Manager administrator password. For example:

```
Prompt> ./LDAPConfigPreSetup.sh
[Enter OID admin password:]
[Enter OIM admin password:]
```

Note: The OIM Admin Password provided here is for the oimadmin user that is created in OID and used for LDAP sync operations.

The Output will be similar to this:

```
./LDAPConfigPreSetup.sh
[Enter OID admin password:]
[Enter OIM admin password:]
Jun 21, 2010 6:16:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ./oimadminuser.ldif
Jun 21, 2010 6:16:20 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ./oimcontainers.ldif
Jun 21, 2010 6:16:20 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ../../oam/server/oim-intg/schema/OID_oblix_schema_add.ldif
Jun 21, 2010 6:16:48 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ../../oam/server/oim-intg/schema/OID_oblix_schema_index_
```

add.ldif

```

Jun 21, 2010 6:26:03 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ../../oam/server/oim-intg/schema/OID_oblix_pwd_schema_
add.ldif
Jun 21, 2010 6:26:04 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: ../../oam/server/oim-intg/schema/OID_oim_pwd_schema_add.ldif
    
```

5. Validate that the script completed successfully.

13.3.1.2 Creating Adapters in Oracle Virtual Directory

OIM used OVD to connect to external LDAP stores. You must create a user adapter and a change log adapter in OVD to enable OIM to connect to the external LDAP store like OID. Follow these steps to create the adapters.

User Adapter

Create the user adapter on the OVD instances running on OVDHOST1 and OVDHOST2 individually. Follow these steps to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at <http://admin.mycompany.com/odsm>.
2. Create connections to each of the OVD instances running on OVDHOST1 and OVDHOST2, if they do not already exist
3. Connect to each OVD instance by using the appropriate connection entry.
4. On the Home page, click the **Adapter** tab.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	Adapter Type	LDAP
	Adapter Name	OIM User Adapter
	Adapter Template	User_OID
Connection	Use DNS Setting	No
	Host	oid.mycompany.com
	Port	389
	Server Proxy Bind DN	cn=oimadmin,cn=users,cn=oim,cn=products,cn=oraclecontext
	Proxy Password	oimadmin password. This is same as the password provided in Section 13.3.1.1 .
Connection Test		Validate that the test succeeds.
Namespace	Remote Base	dc=mycompany,dc=com
	Mapped Namespace	dc=mycompany,dc=com

Screen	Field	Value/Step
Summary		Verify that the summary is correct and then click Finish .

6. Edit the User Adapter to match the values shown in the following table.

Parameter	value
directoryType	oid
pwdMaxFailure	10
oamEnabled	True

To edit the user adapter follow these steps:

- a. Select the OIM User Adapter.
- b. Click the **Plug-ins** Tab.
- c. Click the Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
- d. In the Parameters table, update the parameter values if needed.
- e. Click **OK**.
- f. Click **Apply**.

Change Log Adapter

Create the change log adapter on the OVD instances running on OVDHOST1 and OVDHOST2 individually. Follow these steps to create the Change Log Adapter in OVD using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at <http://admin.mycompany.com/odsm>.
2. Create connections to each of the OVD instances running on OVDHOST1 and OVDHOST2, if they do not already exist.
3. Connect to an OVD instance by using the appropriate connection entry.
4. On the Home page, click on the **Adapter** tab.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

Screen	Field	Value/Step
Type	Adapter Type	LDAP
	Adapter Name	OIM Change Log Adapter
	Adapter Template	Changelog_OID
Connection	Use DNS Setting	No
	Host	oid.mycompany.com
	Port	389

Screen	Field	Value/Step
	Server Proxy Bind DN	cn=oimadmin,cn=users,cn=oim,cn=products,cn=oraclecontext
	Proxy Password	oimadmin password. This is same as the password provided in Section 13.3.1.1 .
Connection Test		Validate that the test succeeds.
Naming Space	Remote Base	cn=changelog
Mapped Namespace		cn=changelog
Summary		Verify that the summary is correct, then click Finish .

6. Edit the Change Log Adapter to match the values shown in the following table.

Parameter	Value
directoryType	oid
mapAttribute	targetGUID=orclGUID
mapObjectclass	changelog=changelogentry
requiredAttribute	orclGUID
addAttribute	orclContainerOC,changelogSupported=1
modifierDNFilter	cn=oimadmin,cn=users,cn=OIM,cn=Products,cn=OracleContext
sizeLimit	1000
targetDNFilter	dc=mycompany,dc=com Search based from which reconciliation needs to happen. This value must be the same as the LDAP SearchDN that is specified during OIM installation.
mapUserState	True
oamEnabled	True or false depending on whether OAM integration with OIM is enabled or not.

To edit the change adapter follow these steps.

- a. Select the OIM Change Log Adapter.
- b. Click the **Plug-ins** tab.
- c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click "Edit in the plug-ins table. The plug-in editing window appears.
- d. In the Parameters table, update the parameter values.
- e. Click **OK**.
- f. Click **Apply**.

Stopping and Starting Oracle Internet Directory and Oracle Virtual Directory

Stop and Start:

- The OVD instances running on both OVDHOST1 and OVDHOST2.
- The OID instances running on both OIDHOST1 and OIDHOST2.

as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

13.3.2 Running the Oracle Identity Management Configuration Wizard

You must configure the OIM server instances before you can start the OIM and SOA Managed Servers. The Oracle Identity Management Configuration Wizard loads the OIM metadata into the database and configures the instance.

Make sure that following env variables are not set in the current shell: DOMAIN_HOME, WL_HOME.

Start the Web Logic Administration Server, then follow these steps on IDMHOST1.

The Oracle Identity Management Configuration Wizard is located under the Identity Management Oracle Home. Type:

```
MW_HOME/iam/bin/config.sh
```

Proceed as follows:

1. On the Welcome screen, click **Next**
2. On the Components to Configure screen, Select **OIM Server** and **OIM Remote Manager**.
Click **Next**.
3. On the Database screen, provide the following values:
 - **Connect String:** The connect string for the OIM database. For example:
oimdb1-vip.mycompany.com:1521:oimedg1
oimdb2-vip.mycompany.com:1521:oimedg2@oimedg.mycompany.com
 - **OIM Schema User Name:** *edg_oim*
 - **OIM Schema password:** *password*
 - **MDS Schema User Name:** *edg_mds*
 - **MDS Schema Password:** *password*
 Select **Next**.
4. On the WebLogic Administration Server screen, provide the following details for the WebLogic Admin Server:
 - **URL:** The URL to connect to the WebLogic Administration Server. For example: *t3://adminvhn.mycompany.com:7001*
 - **UserName:** *weblogic*
 - **Password:** Password for the *weblogic* user
 Click **Next**.
5. On the OIM Server screen, provide the following values:
 - **OIM Administrator Password:** Password for the OIM Administrator. This is the password for the *xelsysadm* user.

- **Confirm Password:** Confirm the password.
- **OIM HTTP URL:** Proxy URL for the OIM Server. This is the URL for the Hardware load balancer that is front ending the OHS servers for OIM. For example: `https://sso.mycompany.com:443`.
- **Key Store Password:** Key store password. The password must have an uppercase letter and a number. For example: `MyPassword1`

Click **Next**.

6. On the LDAP Sync and OAM screen, select **Configure BI Publisher** and provide the **BI Publisher URL**:

`http://bipublisher.mycompany.com/bipublisher`.

Select **Enable LDAP Sync**

Notes:

- Do not select **Enable Identity Administration Integration with OAM**. This will be configured later.
 - BI Publisher is not a part of the IDMDomain. The steps to configure the BI Publisher are not covered in this Enterprise Deployment Guide.
-
-

Click **Next**.

7. On the LDAP Server screen, provide the following LDAP server details:

- **LDAP URL :** The URL to access the LDAP server. For example:
`ldap://ovd.mycompany.com:389`
- **LDAP User :** The username to connect to the LDAP Server. For example:
`cn=orcladmin`
- **LDAP Password:** The password to connect to the LDAP server.
- **LDAP SearchDN:** The Search DN. For example: `dc=mycompany, dc=com`.

Click **Next**.

8. On the LDAP Server Continued screen, provide the following LDAP server details:

- **LDAP Role Container:** The DN for the Role Container. This is the container where the OIM roles are stored. For example:
`cn=oimroles, dc=mycompany, dc=com`
- **LDAP User Container:** The DN for the User Container. This is the container where the OIM users are stored. For example: `cn=oimusers, dc=mycompany, dc=com`
- **User Reservation Container:** The DN for the User Reservation Container. For example: `cn=oimreserved, dc=mycompany, dc=com`.

Note: These container values should be the same as those used in `LDAPConfigPreSetup.sh`.

Click **Next**.

9. On the Remote Manager screen, provider the following values:

- **Service Name:** EDG_RManager
 - **RMI Registry Port:** 12345
 - **Listen Port (SSL):** 12346
10. On the Configuration Summary screen, verify the summary information.
Click **Configure** to configure the Oracle Identity Manager instance
 11. On the Configuration Progress screen, once the configuration completes successfully, click **Next**.
 12. On the Configuration Complete screen, view the details of the Oracle Identity Manager Instance configured.
Click **Finish** to exit the Configuration Assistant.

13.4 Propagating the Oracle Identity Manager and SOA Managed Servers to OIMHOST1 and OIMHOST2

Once the configuration has succeeded on IDMHOST1, you can propagate the configuration to OIMHOST1 and OIMHOST2. You do this by packing the domain on IDMHOST1 and unpacking it on OIMHOST1 and OIMHOST2.

Follow these steps to propagate the domain to IDMHOST1.

1. Invoke the `pack` utility from `MW_HOME/oracle_common/common/bin/`.

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/u01/app/oracle/admin/templates/oim_domain.jar -template_name="OIM Domain"
-managed=true
```
2. This creates a file called `oim_domain.jar` in the `/u01/app/oracle/admin/templates` directory. Copy this file to OIMHOST1 and OIMHOST2.
3. On OIMHOST1, invoke the utility `unpack`, which is also located in the directory `MW_HOME/oracle_common/common/bin/`.

```
./unpack.sh -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain
-template=/u01/app/oracle/product/fmw/templates/oim_domain.jar -overwrite_
domain=true -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```
4. On OIMHOST2, invoke the utility `unpack`, which is also located in the directory `MW_HOME/oracle_common/common/bin/`.

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
-template=/tmp/oim_domain.jar -template_name="OIM Domain"
```

13.5 Post-Installation Steps on OIMHOST1 and OIMHOST2

Perform the following post-installation steps.

13.5.1 Updating the Coherence Configuration for the SOA Managed Server

Follow these steps to update the Coherence Configuration for the WLS_SOA Server.

1. Log 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 in the **Name** column of the table. The settings page for the selected server appears.
5. Click the **Server Start** tab.
6. Enter text into the Arguments field for WLS_SOA1 and WLS_SOA2 .

For WLS_SOA1, enter the following text on a single line, without a carriage return:

```
-Dtangosol.coherence.wka1=oimhost1vhn1 -Dtangosol.coherence.wka2=oimhost2vhn1
-Dtangosol.coherence.localhost=oimhost1vhn1
```

For WLS_SOA2, enter the following text on a single line, without a carriage return:

```
-Dtangosol.coherence.wka1=oimhost1vhn1 -Dtangosol.coherence.wka2=oimhost2vhn1
-Dtangosol.coherence.localhost=oimhost2vhn1
```

Note: The Coherence cluster used for deployment uses port 8088 by default. You can change this port by specifying a different port (for example, 8089) with the `-Dtangosol.coherence.wkan.port` and `-Dtangosol.coherence.localport` startup parameters. For example:

For WLS_SOA1 (on a single line):

```
-Dtangosol.coherence.wka1=oimhost1vhn1
-Dtangosol.coherence.wka2=oimhost2vhn1
-Dtangosol.coherence.localhost=oimhost1vhn1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

For WLS_SOA2 (on a single line):

```
-Dtangosol.coherence.wka1=oimhost1vhn1
-Dtangosol.coherence.wka2=oimhost2vhn1
-Dtangosol.coherence.localhost=oimhost2vhn1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

7. Click **Save** and activate the changes.
8. Restart the Oracle SOA Suite servers.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

Do not copy the text from this section to your Administration Console's arguments text field. Doing so can cause HTML tags to be inserted in the Java arguments. The text should not include any text or characters other than the ones shown.

13.5.2 Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1

Follow this sequence of steps to start the WLS_OIM1 Managed Server on OIMHOST1:

1. Stop the WebLogic Administration Server on OIMHOST1 by using the WebLogic Administration Console as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Start the Administration Server on OIMHOST1 using the node manager, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
3. Validate that the Administration Server started up successfully by bringing up the Oracle WebLogic Administration Console.
4. Start NodeManager on OIMHOST1.
5. Start the WLS_SOA1 managed server, using the WebLogic Administration Console as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
6. Start the WLS_OIM1 managed server using the WebLogic Administration Console. The WLS_OIM1 managed server must be started only after starting the WLS_SOA1 managed server.

13.5.3 Validating Oracle Identity Manager Instance on OIMHOST1

Validate the Oracle Identity Manager Server Instance by bringing up the OIM Console in a web browser at: `http://oimhost1.mycompany.com:8001/oim/self`.

Log in using the `xelsysadm` username and password.

Note: When you log in for the first time, you will be prompted to setup Challenge Questions. Please do so before proceeding further.

13.6 Post Installation Steps on OIMHOST2

Perform the following post-installation steps on OIMHOST2.

13.6.1 Starting Node Manager on OIMHOST2

1. Start the Node Manager on OIMHOST2 to create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the `MW_HOME/wlserver_10.3/server/bin` directory.
2. Before you can start the managed servers by using the console, node manager requires that the property `StartScriptEnabled` is set to `true`. You set it by running the `setNMProps.sh` script located under the `MW_HOME/oracle_common/common/bin` directory.

```
prompt> $MW_HOME/oracle_common/common/bin
prompt> ./setNMProps.sh
```

3. Stop and Start the node manager as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) so that the properties take effect.

13.6.2 Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2

Follow this sequence of steps to start the WLS_OIM1 Managed Server on OIMHOST1:

1. Validate that the Administration Server started up successfully by bringing up the Administration Console.
2. Start the WLS_SOA1 managed server using the WebLogic Administration Console.
3. Start the WLS_OIM1 managed server using the WebLogic Administration Console. The WLS_OIM1 managed server must be started only after starting the WLS_SOA1 managed server

13.6.3 Validating Oracle Identity Manager Instance on OIMHOST2

Validate the Oracle Identity Manager Server Instance by bringing up the OIM Console in a web browser at: `http://oimhost2.mycompany.com:8001/oim/`.

Log in using the `xelsysadm` username and password

13.7 Configuring Oracle Internet Directory using the LDAP Configuration Post setup Script

The OIM LDAP configuration post-setup script updates the OIM LDAP Sync scheduled jobs with the last change number from OID. The LDAP configuration post-setup script is located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory. To run the script, follow these steps:

1. Edit the `ldapconfig.props` file located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory and provide the following values:
 - **OIMProviderURL:**
"t3://oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000"
 - **OIDURL:** `ldap://oidhost1.mycompany.com:389`
 - **OIDAdminUsername:** `cn=orcladmin`
 - **OIDSearchBase:** `mycompany.com`
 - **UserContainerName :** `cn=OIMUsers`
 - **RoleContainerName:** `cn=OIMRoles`
 - **ReservationContainerName:** `cn=OIMReserve`

Note: `usercontainerName`, `rolecontainername`, and `reservationcontainername` are not used in this step.

2. Save the file.
3. Set the `WL_HOME` and `JAVA_HOME` environment variables.
4. Run `LDAPConfigPostSetup.sh`. The script prompts for the OID Admin Password and the OIM Admin Password. For example:

```
Prompt> ./LDAPConfigPostSetup.sh
[Enter OID admin password: ]
[Enter OIM admin password: ]
```

13.8 Configuring Oracle Identity Manager to Work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier

13.8.1 Prerequisites

Before configuring Oracle Access Manager to work with the Oracle Web Tier, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on `WEBHOST1` and `WEBHOST2`.
2. Install and configure Oracle Access Manager on `IDMHOST1` and `IDMHOST2`.
3. Configure the load balancer with a virtual hostname (`sso.mycompany.com`) pointing to the web servers on `WEBHOST1` and `WEBHOST2`.
4. Configure the load balancer with a virtual hostname (`admin.mycompany.com`) pointing to web servers `WEBHOST1` and `WEBHOST2`.

13.8.2 Configuring Oracle HTTP Servers to front end the OIM & SOA Managed Servers.

1. On each of the web servers on `WEBHOST1` and `WEBHOST2`, create a file called `oim.conf` in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. This file must contain the following information:

```
# oim admin console(idmshell based)
<Location /admin>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim self and advanced admin webapp consoles(canonic webapp)

<Location /oim>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
<Location /sodcheck>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster oimhost1.us.oracle.com:8001,oimhost2.us.oracle.com:8001
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Callback webservice for SOA. SOA calls this when a request is
approved/rejected
# Provide the SOA Managed Server Port
<Location /workflowservice>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
```

```

        WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
    SetHandler weblogic-handler
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
    SetHandler weblogic-handler
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# used for FA Callback service.
<Location /callbackResponseService>
    SetHandler weblogic-handler
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# spml xsd profile
<Location /spml-xsd>
    SetHandler weblogic-handler
    WLCookieName    oimjsessionid
    WebLogicCluster oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

<Location /HTTPClnt>
    SetHandler weblogic-handler
    WLCookieName    oimjsessionid
    WebLogicCluster
oimhost1.us.oracle.com:14000,oimhost2.us.oracle.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

```

2. Save the file on both WEBHOST1 and WEBHOST2.
3. Stop and start the Oracle HTTP Server instances on both WEBHOST1 and WEBHOST2 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

13.8.3 Validating Oracle Identity Manager Instance from the WebTier

Validate the OIM Server Instance by bringing up the OIM Console in a web browser. at: <http://sso.mycompany.com/oim>. Log in using the xelsysadm username and password.

13.9 Configuring a Shared JMS Persistence Store

Configure the location for all of the persistence stores as a directory that is visible from both nodes. See [Section 2.4, "Shared Storage and Recommended Directory Structure"](#) for more information. Change all of the persistent stores to use this shared base directory as follows:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Lock and Edit**.
3. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node. The Summary of Persistence Stores page is displayed.
4. Select the persistence store (represented as a hyperlink) from the **Name** column of the table. The Settings page for the persistence store is displayed.
5. On the **Configuration** tab, in the **Directory** field, enter the location of a persistent storage solution (such as NAS or SAN) that is available to other servers in the cluster. Specifying this location enables pending JMS messages to be sent.
6. The location should have the following directory structure.

For the WLS_SOA1 and WLS_SOA2 servers, use a directory structure similar to `ORACLE_BASE/admin/domain_name/soa_cluster_name/jms`.

For the WLS_OIM1 and WLS_OIM2 servers use a directory structure similar to `ORACLE_BASE/admin/domain_name/oim_cluster_name/jms`.

Note:

- The WLS_OIM1 and WLS_OIM2 servers must be able to access this directory.
 - The WLS_SOA1 and WLS_SOA2 servers must be able to access this directory.
 - This directory must also exist before you restart the server.
-
-

7. Click **Save**.
8. Click **Activate Changes** from the change center.
9. Do not restart the OIM and SOA managed servers. They will be restarted after performing the steps in [Section 13.10, "Configuring a Default Persistence Store for Transaction Recovery."](#)

13.10 Configuring a Default Persistence Store for Transaction Recovery

The WLS_OIM and WLS_SOA Managed Servers have a transaction log that stores information about committed transactions that are coordinated by the server that might not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

Note: Preferably, this location should be on a dual-ported SCSI disk or on a Storage Area Network (SAN).

Perform these steps to set the location for the default persistence stores for the OIM and SOA Servers:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Lock and Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.
The Summary of Servers page is displayed.
4. Click the name of the server (represented as a hyperlink) in the **Name** column of the table.
5. The Settings page for the selected server is displayed, and defaults to the **Configuration** tab.
6. Open the **Services** sub tab.
7. In the **Default Store** section of the page, enter the path to the folder where the default persistent stores will store its data files. The directory structure of the path is as follows:
 - For OIM Servers: `ORACLE_BASE/admin/domain_name/oim_cluster_name/tlogs`
 - For SOA Servers: `ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs`
8. Click **Save and Activate**.
9. Restart the OIM and SOA managed servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) to make the changes take effect.

Note: To enable migration of the Transaction Recovery Service, specify a location on a persistent storage solution that is available to other servers in the cluster. All the servers that are a part of the cluster must be able to access this directory.

13.11 Adding the CSF Entries for Oracle Identity Management and WSM

If you extend your domain with Oracle Identity Manager after the domain has been associated with an external LDAP store, the OIM configuration wizard does not populate the Credential Store Framework with the appropriate key-value pairs required for the Oracle Identity Manager and Oracle SOA Suite managed servers to start up. To work around this issue, you must create the required entries manually, by using Oracle Enterprise Manager Fusion Middleware Control. This is a temporary workaround.

Follow these steps to create the entries:

1. Open a browser and bring up Fusion Middleware Control at:
`http://admin.mycompany.com/em`.
2. Log in as the Weblogic user.
3. Expand `Farm_DomainName` in the left pane and navigate to **Weblogic Domain > Domain Name**. For Example if `IDMDomain` is the name your domain, navigate to **Farm_IDMDomain > Weblogic Domain > IDMDomain**
4. The IDMDomain Page appears in the right pane.

5. Navigate to **Weblogic Domain > Security > Credential** to bring up the Credentials Page.
6. On the Credentials page, Click **Create Map** to create a map. Create a map called `oim` for the Oracle Identity Manager entries and a map called `oracle.wsm.security` for the WSM entries.
7. Create the entries for the maps in the table. Select the map where you want to add entries and click **Create Key** to create a key.

Enter the following values on the Create Key page:

- **Select Map:** Map Name
- **Key:** Key Name
- **Type:** Password
- **User Name:** User Name
- **Password:** Password
- **Description:** Description for the Key

Click **OK**.

Refer to the following table to create the keys required for Oracle Identity Manager and the `oracle.wsm.security` maps.

Select Map	Key	Type	User Name	Password
oim	OIMSchemaPassword	Password	OIMSchemaPassword	Password for OIM DB
oim	xell	Password	xell	Password for Keystore
oim	DataBaseKey	Password	DataBaseKey	Password for Keystore
oim	JMSKey	Password	JMSKey	Password for Keystore
oim	.xldatabasekey	Password	.xldatabasekey	Password for Keystore
oim	default-keystore.jks	Password	default-keystore.jks	Password for Keystore
oim	SOAdminPassword	Password	SOAdminPassword	Password for Keystore
oracle.wsm.security	keystore-csf-key	Password	owsm	Password for weblogic user
oracle.wsm.security	enc-csf-key	Password	xell	Password for Keystore
oracle.wsm.security	sign-csf-key	Password	xell	Password for Keystore
oracle.wsm.security	recipient-alias-key	Password	xell	not used

Password For Key Store is the key store password provided when running the OIM Configuration Wizard

8. Stop and Start the Administration Server.

9. Start the Oracle Identity Management and Oracle SOA Suite Managed Servers using the WebLogic Admin Console.
10. The Oracle Identity Management and Oracle SOA Suite Managed Servers start up correctly after you create the maps.

Extending the Domain with Authorization Policy Manager and Identity Navigator

This chapter covers the following topics:

- [Section 14.1, "Extending the Domain with Oracle Authorization Policy Manager"](#)
- [Section 14.2, "Extending the Domain with Oracle Identity Navigator"](#)

14.1 Extending the Domain with Oracle Authorization Policy Manager

Oracle Authorization Policy Manager (APM) is the single centralized console for managing authorization for Fusion applications/J2EE applications and Oracle Fusion Middleware components that provide various services to those applications. An application administrator has a single console for administering various Authorization polices for an application.

You can use either WLST commands or Fusion Middleware Control to manage application policies. Using WLST command requires manually running commands. Fusion Middleware Control offers a graphical user interface, but it is a rather complex tool. It requires you to work with low-level security artifacts and to know names and concepts used by developers, such as permission class names or task-flow names.

Authorization Policy Manager greatly simplifies the creation, configuration, and administration of application policies over those two other tools by providing the following features:

- User-friendly names and descriptions of security artifacts. For details, see the "OPSS Authorization Model" chapter in the *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*.
- A way to organize application roles by business, product, or any other parameter specific to an application. For details, see the "Role Categories" section in the *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*.
- A uniform graphic interface to search, create, browse, and edit security artifacts. For details, see the "Querying Security Artifacts, and "Managing Security Artifacts" chapters in the *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*.
- A way to specify a subset of applications that a role can manage. For details, see the "Delegated Administration" chapter in the *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*.

14.1.1 Base Authorization Policy Manager Platform

The APM Console enables an APP administrator to manage following artifacts at a high level when it comes to authorization.

1. External Roles
2. Application Roles
3. Resources–Target
4. Policy–Subject, Target, Grants

Other artifacts include:

1. Entitlements (aggregation of resources)
2. Resource types (metadata definition for resources)
3. Role templates (role generation based on templates with template policies)

Note: The administration of these artifacts varies. For example, creation of enterprise roles is done externally in an identity and provisioning system. APM will only provide read level services for Enterprise Roles.

14.1.2 Prerequisites

Before configuring Authorization Policy Manager, ensure that the following tasks have been performed:

1. Install the following software on IDMHOST1 and IDMHOST2 as described in [Chapter 4](#).
 - Oracle WebLogic Server
 - Oracle Identity and Access Management
2. Make sure that the APM schema was created by following the steps in [Chapter 3](#).

14.1.3 Configuring Authorization Policy Manager on IDMHOST1

Start the configuration wizard by executing the command:

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

Then proceed as follows:

1. On the Welcome Screen, select **Extend an Existing WebLogic Domain**. Click **Next**
2. On the screen Select a WebLogic Domain, using the Navigator, select the domain home of the admin server, for example:

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

Click **Next**

3. On the Select Extension Source screen, select **Oracle Authorization Policy Manager**. Click **Next**.
4. The Configure RAC Multi Datasources screen shows the Multi Datasources for previously configured components in your domain. Do not make any changes. Click **Next**.

5. On the Configure JDBC Component Schema screen, select **Configure selected Component schemas as RAC multi data source schemas** in the next panel. Click **Next**
6. On the screen Configure RAC Multi Data Source Component Schemas, select all the Multi Data source Schemas and enter the following:
 Service Name: For example, `idmedg.us.oracle.com`
 For the First RAC Node, enter:
 - **HostName:** For example, `idmdb1.us.oracle.com`
 - **Instance Name:** For example, `idmedg1`
 - **Port:** For example, `1521`
 Click **Add** to add an additional row.
 For the second RAC Node, enter
 - **HostName:** For example, `idmdb2.us.oracle.com`
 - **Instance Name:** For example, `idmedg2`
 - **Port:** For example, `1521`
 Select **APM MDS Schema** and Enter the UserName and Password. For example:
`EDG_MDS password`
7. On the Test Component Schema screen, select **All the Schemas** and then click **Test Connections**. Validate that the test for all the schemas completed successfully. Click **Next**.
8. On the Select Optional Configuration screen, do not make any selections. Click **Next**.
9. On the Configuration Summary screen, click **Extend** to extend the domain.
10. On the Extending Domain screen, click **Done** to exit the Configuration Wizard.

14.1.4 Stopping and Starting the Admin Server IDMHOST1

In this Enterprise Deployment Topology, APM is being deployed to the Administration Server. To complete the deployment of APM, stop and start WebLogic Administration Server on IDMHOST1 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

Validating Authorization Policy Manager

Validate the implementation using the APM Console, at `http://ADMINVH.mycompany.com:7001/apm`.

The APM console login page is displayed. Log in using the WebLogic administrator credentials.

14.1.5 Authorization Policy Manager on IDMHOST2

In this Enterprise Deployment Topology, APM is deployed to the Administration Server in an active-passive configuration. Because APM is failed over along with the Administration Server, there is no need to provision APM on IDMHOST2.

Follow the steps in [Section 6.13, "Manually Failing Over the Administration Server"](#) to fail over APM from IDMHOST1 to IDMHOST2.

14.1.6 Configure Oracle HTTP Servers to Access Authorization Policy Manager Console

On each of the web servers on WEBHOST1 and WEBHOST2, a file called `admin.conf` was created in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. (See [Section 6.9, "Configuring Oracle HTTP Server for the Administration Server"](#).)

Edit `admin.conf` and add the following lines inside the `virtual host` definition:

```
<Location /apm>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>
```

After editing the file should look like this:

```
NameVirtualHost *:80

<VirtualHost *:80>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

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

<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

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

<Location /apm>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>

</VirtualHost>
```

Restart the Oracle HTTP Server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.1.6.1 Validating the Implementation

Validate the implementation using the APM Console at `http://admin.mycompany.com:7001/apm`. The APM console login page is displayed. Log in using the WebLogic administrator's credentials.

14.1.7 Configuring Authorization Policy Manager to Use an External LDAP Store

By default, Oracle WebLogic Server uses the local LDAP store that is created as part of the installation and configuration process. Typically, enterprise deployments require a centralized LDAP store to provision users, groups, roles, and policies, so you must configure Oracle WebLogic Server to use an external LDAP store, such as Oracle Internet Directory. Configuring APM with an external LDAP store is covered in [Chapter 17, "Integrating Components."](#) Please refer to [Section 17.1, "Migrating Policy and Credential Stores"](#) for the steps on Configuring APM to use an External LDAP Store.

14.2 Extending the Domain with Oracle Identity Navigator

Oracle Identity Navigator is an administrative portal designed to act as a launch pad for Oracle Identity Management components. It allows you to access the Oracle Identity Management consoles from one site. It is installed with other Oracle Identity Management components, and enables you access other components by product discovery.

Oracle Identity Navigator is a J2EE application deployed on a Oracle WebLogic Administration Server. It uses Oracle Metadata Service.

The Oracle Identity Navigator report feature relies on Oracle Business Intelligence Publisher.

14.2.1 Prerequisites

Install Software on IDMHOST1 and IDMHOST2

Install the following software on IDMHOST1 and IDMHOST2 as described in [Chapter 4](#).

1. Oracle WebLogic Server
2. Oracle Identity and Access Management

14.2.2 Configure Oracle Identity Navigator on IDMHOST1

Start the configuration wizard by executing the command:

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

Then proceed as follows:

1. On the Welcome Screen, select **Extend an Existing WebLogic Domain**. Click **Next**
2. On the screen Select a WebLogic Domain, using the Navigator, select the domain home of the administration server, for example:

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

Click **Next**

3. On the Select Extension Source screen, select **Oracle Identity Navigator**. Click **Next**

4. The Configure RAC Multi Datasources screen shows the Multi Datasources for previously configured components in your domain. Do not make any changes. Click **Next**.
5. On the Select Optional Configuration screen, do not make any selections. Click **Next**.
6. On the Configuration Summary screen, click **Extend** to extend the domain.
7. On the Extending Domain screen, click **Done** to exit the Configuration Wizard.

14.2.3 Stopping and Starting the Administration Server IDMHOST1

Stop and Start WebLogic Admin Server on IDMHOST1 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.2.4 Provisioning Oracle Identity Navigator on IDMHOST1

In this Enterprise Deployment Topology, Oracle Identity Navigator is deployed to the Admin Server in an active-passive model. Since Oracle Identity Navigator is failed over along with the Admin Server, there is no need to provision Oracle Identity Navigator on IDMHOST2.

Follow the steps in [Section 6.13, "Manually Failing Over the Administration Server"](#).

14.2.5 Configuring Oracle HTTP Servers to Access Oracle Identity Navigator Console

On each of the web servers on WEBHOST1 and WEBHOST2, a file called `admin.conf` was created in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. (See [Section 6.9, "Configuring Oracle HTTP Server for the Administration Server"](#).)

Edit `admin.conf` and add the following lines in the virtual host definition:

```
<Location /oinav>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>
```

After editing the file should look like this:

```
NameVirtualHost *:80

<VirtualHost *:80>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

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

<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
```

```
WebLogicPort 7001
</Location>

<Location /em>
SetHandler weblogic-handler
WebLogicHost ADMINVHN
WebLogicPort 7001
</Location>

<Location /apm>
  SetHandler weblogic-handler
  WebLogicHost ADMINVHN
  WebLogicPort 7001
</Location>

<Location /oinav>
  SetHandler weblogic-handler
  WebLogicHost ADMINVHN
  WebLogicPort 7001
</Location>

</VirtualHost>
```

Restart the Oracle HTTP Server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.2.6 Validating Oracle Identity Navigator

Validate the implementation using the Oracle Identity Navigator Console at `http://admin.mycompany.com:7001/oinav`. The Oracle Identity Navigator login page is displayed. Log in using the WebLogic administrator's credentials.

Extending the Domain with Oracle Identity Federation

This chapter contains the following topics:

- [Section 15.1, "Prerequisites"](#)
- [Section 15.2, "Configuring Oracle Identity Federation on OIFHOST1"](#)
- [Section 15.3, "Configuring Oracle Identity Federation on OIFHOST2"](#)
- [Section 15.4, "Post-Installation Steps for Oracle Identity Federation"](#)
- [Section 15.5, "Provisioning the Managed Servers on the Local Disk"](#)
- [Section 15.6, "Enabling Oracle Identity Federation Integration with LDAP Servers"](#)
- [Section 15.7, "Configuring Oracle Identity Federation to work with the Oracle Web Tier"](#)
- [Section 15.8, "Validating"](#)

Oracle Identity Federation is a self-contained, standalone federation server that enables single sign-on and authentication in a multiple-domain identity network and supports the broadest set of federation standards. This allows users to federate in heterogeneous environments and business associations, whether they have implemented other Oracle Identity Management products in their solution set or not.

It can be deployed as a multi-protocol hub acting as both an Identity Provider (IdP) and Service Provider (SP).

Acting as an SP, Oracle Identity Federation enables you to manage your resources while off loading actual authentication of users to an IdP, without having to synchronize users across security domains out of band. Once authenticated at the IdP, the SP can allow or deny access to users for the SP's applications depending upon the local access policies.

15.1 Prerequisites

Before proceeding with Oracle Identity Federation configuration, ensure that the following tasks have been performed.

1. Installing and upgrading the software on OIFHOST1 and OIFHOST2 as described in [Section 4.5.3](#), [Section 4.5.4](#), and [Section 4.6.1](#).
2. Running the Repository Creation Utility (RCU) to create and configure the collection of schemas used by OIF as described in [Chapter 3](#).
3. Creating the Identity Management Domain as described in [Chapter 6](#).

4. Installing and configuring Oracle Internet Directory as described in [Chapter 7](#). Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory is used as the User Store and the Federation Store
5. Installing and configuring Oracle HTTP Server on WEBHOST1 and WEBHOST2 as described in [Chapter 5](#)
6. Associating the Identity Management Domain created with an External LDAP Store as described in [Section 17.1](#). This is required because Oracle Identity Federation is being extended on a node where the Administration Server is not running.

15.2 Configuring Oracle Identity Federation on OIFHOST1

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

2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 2.4](#), "Shared Storage and Recommended Directory Structure."

On UNIX:

- 1.
- 2.
3. Ensure that port 7499 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

```
netstat -an | grep "7499"
```

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

On UNIX:

Remove the entries for port 7499 in the `/etc/services` file and restart the services, as described in [Section 18.1](#), "Starting and Stopping Oracle Identity Management Components," or restart the computer.

4. If you plan to provision the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 2.4](#), "Shared Storage and Recommended Directory Structure."
5. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.
6. Edit the `staticports.ini` file that you copied to the temporary directory to assign the following custom port:

```
#The port for OIF Server port  
OIF Server Port No = 7499
```

7. Start the Oracle Identity Management 11g Configuration Assistant located under the `ORACLE_HOME/bin` directory as follows:

On UNIX, issue this command:

```
./config.sh
```

On Windows, double-click `config.exe`

8. On the Welcome screen, click **Next**.
9. On the Select Domain screen, select Extend Existing Domain and specify these values:
 - **HostName:** `adminvhn.mycompany.com`
 - **Port:** `7001`
 - **UserName:** `weblogic`
 - **User Password:** `weblogic_user_password`

Click **Next**.

10. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

This is a benign warning that you can ignore.

Click **Yes** to continue.

11. On the Specify Installation Location screen, specify the following values:
 - **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`
This value is prefilled and cannot be updated.
 - **Oracle Home Directory:** `idm`
This value is prefilled and cannot be updated
 - **WebLogic Server Directory:**
`/u01/app/oracle/product/fmw/wlserver_10.3`
 - **Oracle Instance Location:** `/u01/app/oracle/admin/oif_inst1`
 - **Instance Name:** `oif_inst1`

Note: Ensure that the Oracle Home Location directory path for OIFHOST1 is the same as the Oracle Home Location path for OIFHOST2. For example, if the Oracle Home Location directory path for OIFHOST1 is: `/u01/app/oracle/product/fmw/oif`, then the Oracle Home Location directory path for OIFHOST2 must also be `/u01/app/oracle/product/fmw/oif`.

Click **Next**.

12. On the Specify Oracle Configuration Manager Details screen, specify the values shown in the example below:
 - **Email Address:** Provide the email address for your My Oracle Support account.

- **Oracle Support Password:** Provide the password for your My Oracle Support account.
- Select **I wish to receive security updates via My Oracle Support**.

Click **Next**.

13. On the Configure Components screen, de-select all the components except Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select Oracle HTTP Server. Select **Clustered**.

Click **Next**.

14. On the Configure Ports screen, select Specify Ports using Configuration File. Provide the path to the staticports.ini file that you copied to the temporary directory.

Click **Next**.

15. On the Specify OIF Details screen, specify these values:

- **PKCS12 Password:** *password*
- **Confirm Password:** Confirm the password
- **Server Id:** oif_server1

Click **Next**.

16. On the Select OIF Advanced Flow Attributes screen, specify these values:

- **Authentication Type:** LDAP
- **User Store:** LDAP
- **Federation Store:** LDAP
- **User Session Store:** RDBMS (default selection, which cannot be changed for a cluster)
- **Message Store:** RDBMS (default selection, which cannot be changed for a cluster).
- **Configuration Store:** RDBMS (default selection, which cannot be changed for a cluster).

Note: When you choose RDBMS for the session, message, and configuration data stores during an Advanced installation, the installer creates one data source for all three data stores. If you want to have separate databases for each of these stores, you must configure this after the installation.

Click **Next**.

17. On the Authentication LDAP Details screen, specify the following values:

- **LDAP Type:** Select **Oracle Internet Directory** from the drop down.
- **LDAP URL:** The LDAP URL to connect to your LDAP store in the format: ldap://host:port or ldaps://host:port. For example: ldaps://oid.mycompany.com:636
- **LDAP Bind DN:** cn=orcladmin

- **LDAP Password:** *orcladmin_password*
- **User Credential ID Attribute:** *uid*
- **User Unique ID Attribute:** *orclguid*
- **Person Object Class:** *inetOrgPerson*
- **Base DN:** *dc=us,dc=oracle,dc=com*

Click Next.

18. On the LDAP Attributes for User Data Store screen, specify the following values:

- **LDAP Type:** Select **Oracle Internet Directory** from the drop down.
- **LDAP URL:** The LDAP URL to connect to your LDAP store in the following format: *ldap://host:port* or *ldaps://host:port*. For example: *ldaps://oid.mycompany.com:636*
- **LDAP Bind DN:** *cn=orcladmin*
- **LDAP Password:** *orcladmin_password*
- **User Description Attribute:** *uid*
- **User ID Attribute:** *orclguid*
- **Person Object Class:** *inetOrgPerson*
- **Base DN:** *dc=mycompany,dc=com*

Click Next.

19. On the LDAP Attributes for Federation Data Store screen, specify the following values:

- **LDAP Type:** Select **Oracle Internet Directory** from the drop down.
- **LDAP URL:** Provide the LDAP URL to connect to your LDAP store in the following format: *ldap://host:port* or *ldaps://host:port*. For example: *ldaps://oid.mycompany.com:636*
- **LDAP Bind DN:** *cn=orcladmin*
- **LDAP Password:** *orcladmin_password*
- **User Federation Record Context:** *cn=myfed,dc=mycompany,dc=com*
- **Container Object Class:** The type of User Federation Record Context that Oracle Identity Federation should use when creating the LDAP container, if it does not exist already. If that field is empty, its value will be set to *applicationprocess*. For Microsoft Active Directory this field must be set to *container*.

Click Next.

20. On the Transient Store Database Details screen, specify the values shown in the example below:

- **Host Name:** The connect string to your database. For example:
infradbhost1-vip.mycompany.com:1521:ldmdb1^infradbhost2-vip.mycompany.com:1521:ldmdb2@idmedg.mycompany.com

Note: The Oracle RAC database connect string information needs to be provided in the format
`host1:port1:instance1^host2:port2:instance2@service_name`. During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed. It is required that the information provided above is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances. Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.

- **UserName:** The username for the OIF Schema. For example: `edg_oif`
- **Password:** `oif_user_password`

Click **Next**.

21. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.
22. On the Configuration Progress screen, view the progress of the configuration.
23. On the Configuration Complete screen, click **Finish** to confirm your choice to exit.

15.3 Configuring Oracle Identity Federation on OIFHOST2

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. If you plan to provision the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)
3. Ensure that port 7499 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

```
netstat -an | grep "7499"
```

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

On UNIX:

Remove the entries for port 7499 in the `/etc/services` file and restart the services, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

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

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

```
#The port for OIF Server port
OIF Server Port No = 7499
```

6. Start the Oracle Identity Management 11g Configuration Assistant located under the `ORACLE_HOME/bin` directory as follows:

On UNIX, issue this command:

```
./config.sh
```

On Windows, double-click `config.exe`

7. On the Welcome screen, click **Next**.
8. On the Select Domain screen, select the **Expand Cluster** option and specify these values:

- **HostName:** ADMINVHN.mycompany.com
- **Port:** 7001
- **UserName:** weblogic
- **User Password:** *weblogic_user_password*

Click **Next**.

9. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

This is a benign warning that you can ignore.

Click **Yes** to continue.

10. On the Specify Installation Location screen, specify the following values:
 - **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw` (This value is prefilled and cannot be updated.)
 - **Oracle Home Directory:** `oif` (This value is prefilled and cannot be updated.)
 - **WebLogic Server Directory:**
`/u01/app/oracle/product/fmw/wlserver_10.3`
 - **Oracle Instance Location:** `/u01/app/oracle/admin/oif_inst2`
 - **Instance Name:** `oif_inst2`

Note: Ensure that the Oracle Home Location directory path for OIFHOST1 is the same as the Oracle Home Location path for OIFHOST2. For example, if the Oracle Home Location directory path for OIFHOST1 is: `/u01/app/oracle/product/fmw/oif`, then the Oracle Home Location directory path for OIFHOST2 must also be `/u01/app/oracle/product/fmw/oif`.

Click **Next**.

11. On the Specify Oracle Configuration Manager Details screen, specify the following values:

- **Email Address:** The email address for your My Oracle Support account
- **Oracle Support Password:** The password for your My Oracle Support account
- **Select: I wish to receive security updates via My Oracle Support**

Click **Next**.

12. On the Configure Components screen, de-select all the components except for Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select **Oracle HTTP Server**.

Click **Next**.

13. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.
14. On the Configuration Progress screen, view the progress of the configuration.
15. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

15.4 Post-Installation Steps for Oracle Identity Federation

Follow the post-installation steps in this section to complete the installation and configuration of the Oracle Identity Federation application

15.4.1 Copying the Oracle Identity Federation Configuration Directory from OIFHOST1 to OIFHOST2

Copy the Oracle Identity Federation configuration directory from OIFHOST1 to OIFHOST2. That is, copy the directory:

```
MW_HOME /user_
projects/domains/IDMDomain/config/fmwconfig/servers/wls_
oif1/applications
```

on:

```
OIFHOST1
```

to:

```
MW_HOME/user_
projects/domains/IDMDomain/config/fmwconfig/servers/wls_
oif2/applications
```

on:

```
OIFHOST2.
```

For example, from OIFHOST1, execute the following is command:

```
scp -rp MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers/wls_
oif1/applicationsuser@OIFHOST2:/MW_HOME/user_
projects/domains/IDMDomain/config/fmwconfig/servers/wls_oif2/applications
```


15.4.2 Set the Listen Address for the Managed Servers

Set the listen address for the `WLS_OIF1` and `WLS_OIF2` Managed Servers to the host name of their respective nodes using the Oracle WebLogic Administration Server:

1. Using a web browser, bring up the Oracle WebLogic Administration Server console and log in using the `weblogic` user credentials.
2. In the left pane of the WebLogic Administration Server Console, click **Lock & Edit** to edit the server configuration.
3. In the left pane of the WebLogic Server Administration Console, expand **Environment** and select **Servers**.
4. On the Summary of Servers page, click the link for the `wls_oif1` Managed Server.
5. On the Settings page for the `wls_oif1` Managed Server, update the **Listen Address** to `oifhost1.mycompany.com`. This is the host name of the server where `wls_ods1` is running.
6. Click **Save** to save the configuration.
7. Repeat Steps 2 to 6 to update the Listen Address for the `wls_oif2` Managed Server to `oifhost2.mycompany.com`. This is host name of the server where `wls_oif2` is running.
8. Click **Activate Changes** to update the server configuration.

15.4.3 Starting the Managed Server on OIFHOST2

Follow these steps to start the newly created `wls_oif2` Managed Server in a cluster on OIFHOST2:

1. In the left pane of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Clusters**.
2. Click the cluster (`cluster_oif`) containing the Managed Server (`wls_oif2`) you want to stop.
3. Select **Control**.
4. Under Managed Server Instances in this Cluster, select the Managed Server (`wls_oif2`) you want to start and click **Start**.
5. On the **Cluster Life Cycle Assistant** page, click **Yes** to confirm.

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

15.5 Provisioning the Managed Servers on the Local Disk

Due to certain limitations, the Oracle Configuration Wizard creates the domain configuration under the `ORACLE_HOME`. In this EDG, the Oracle Home is on shared disk and it is a best practice recommendation to separate the domain configuration from the Oracle Home. This section provides the steps to separate the domain. Proceed as follows:

1. Stop the Administration Server and the Managed Servers (`wls_ods1` and `wls_ods2`) as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

- On `IDMHOST1`, pack the Managed Server domain using the pack command located under the `ORACLE_HOME/common/bin` directory. Make sure to pass the `managed=true` flag to pack the managed server. Type:

```
ORACLE_HOME/common/bin/pack.sh -managed=true \
  -domain=path_to_adminServer_domain -template=templateName.jar \
  -template_name=templateName
```

For example

```
ORACLE_HOME/common/bin/pack.sh -managed=true \
  -domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain \
  -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
  -template_name=ManagedServer_Template
```

- Copy the Managed Server template directory from `IDMHOST1` to both `OIFHOST1` and `OIFHOST2`. For Example:

Copy to `OIFHOST1`:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@OIFHOST1://u01/app/oracle/products/fmw/templates
```

Copy to `OIFHOST2`:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@OIFHOST2://u01/app/oracle/products/fmw/templates
```

- Unpack the Managed Server to the local disk on `OIFMHOST1` using the unpack command located under the `ORACLE_COMMON_HOME/common/bin` directory.

```
ORACLE_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
  -template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_HOME/common/bin/unpack.sh \
  -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
  -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
  -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```

- Unpack the Managed Server to the local disk on `IDMHOST2` using the unpack command located under the `ORACLE_HOME/common/bin` directory.

```
ORACLE_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
  -template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_HOME/common/bin/unpack.sh \
  -domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
  -template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
  -app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```

- Start the Node Manager on `OIFHOST1` and `OIFHOST2` using the `startNodeManager.sh` script located under the `WL_HOME/server/bin` directory. For Example:

```
/u01/app/oracle/product/fmw/wlserver_10.3/server/bin/startNodeManager.sh >
/tmp/nm.log &
```

- Start the Administration server by following the steps in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

8. Validate that the Administration Server started up successfully by opening a browser accessing the Administration Console at `http://ADMINVHN.us.oracle.com:7001/console`.
Also validate Enterprise Manager by opening a browser and accessing Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.us.oracle.com:7001/em`.
9. Start the Managed Servers on `IDMHOST1` and `IDMHOST2` by using the Administration Console. Follow the steps in the Starting Managed Servers section.
10. Delete the `MW_HOME/user_projects` directory on `OIFHOST1` and `OIFHOST2`. This directory is created by the Oracle Universal Installer when the domain is originally configured and is no longer required after the provisioning the Managed Server to the local disk.

15.6 Enabling Oracle Identity Federation Integration with LDAP Servers

By default, Oracle Identity Federation is not configured to be integrated with LDAP Servers deployed in a high availability configuration. To integrate Oracle Identity Federation with highly available LDAP Servers to serve as user data store, federation data store, or authentication engine, you must configure Oracle Identity Federation based on the LDAP server's function.

Enter the WLST script environment for Oracle Identity Federation, then set the following properties as needed:

- To integrate the user data store with a highly available LDAP Server, set the `userldapenabled` boolean property from the `datastore` group to `true`; otherwise set it to `false`:

```
setConfigProperty('datastore','userldapenabled','true','boolean')
```
- To integrate the federation data store with a highly available LDAP Server, set the `fedldapenabled` boolean property from the `datastore` group to `true`; otherwise set it to `false`:

```
setConfigProperty('datastore','fedldapenabled','true','boolean')
```
- To integrate the LDAP authentication engine with a highly available LDAP Server, set the `ldaphaenabled` boolean property from the `authnengines` group to `true`; otherwise set it to `false`:

```
setConfigProperty('authnengines','ldaphaenabled','true','boolean')
```

15.7 Configuring Oracle Identity Federation to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier

15.7.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Oracle Web Tier has been installed on `WEBHOST1` and `WEBHOST2`.
2. Oracle Access Manager has been installed and configured on `IDMHOST1` and `IDMHOST2`.

3. Loadbalancer has been configured with a virtual hostname (sso.mycompany.com) pointing to the webserver on WEBHOST1 and WEBHOST2.
4. Loadbalancer has been configured with a virtual hostname (admin.mycompany.com) pointing to webserver WEBHOST1 and WEBHOST2.

15.7.2 Making OIF aware of the Load Balancer

To configure the Oracle Identity Federation application to use the load balancer VIP, follow these steps:

1. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control, select **Administration**, and then **Server Properties**.
2. Change the host name and port to reflect the load balancer host and port.
3. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control, select **Administration**, and then **Identity Provider**.
4. Change the URL to `http://LoadBalancerHost:LoadBalancerPort`.
5. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control, select **Administration**, and then **Service Provider**.
6. Change the URL to `http://LoadBalancerHost:LoadBalancerPort`.
7. Repeat these steps for each Managed Server where Oracle Identity Federation is deployed.

15.7.3 Configuring Oracle HTTP Servers To Front End the OIF Managed Servers

On each of the web servers on WEBHOST1 and WEBHOST2, create a file called `oif.conf` in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. Edit this file and add the following lines:

```
<Location /fed>
SetHandler weblogic-handler
WebLogicCluster oifhost1.mycompany.com:7499,oifhost2.mycompany.com:7499
</Location>
```

Restart the Oracle HTTP Server, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

15.8 Validating

1. If the configuration is correct, you can access the following URLs from a web browser:
 - `https://sso.mycompany.com/fed/sp/metadata`
 - `https://sso.mycompany.com/fed/idp/metadata`
2. Follow the instructions in the "Obtain Server Metadata" and "Add Trusted Providers" sections of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* to import metadata from the Service Provider into the Identity Provider and the Identity Provider metadata into the Service Provider
3. Go to the following URL and do a Single Sign-On operation:

```
http://SP_Host:SP_port/fed/user/testspssso
```

Setting Up Node Manager

This chapter describes how to configure Node Manager in accordance with the EDG recommendations. It contains the following sections:

- [Section 16.1, "About Setting Up Node Manager"](#)
- [Section 16.2, "Changing the Location of the Node Manager Log"](#)
- [Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"](#)
- [Section 16.4, "Starting Node Manager"](#)

16.1 About Setting Up Node Manager

Node Manager enables you to start and stop the administration server and the managed servers.

Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topologies outlined in [Section 1, "Enterprise Deployment Overview."](#) The topologies and hosts are shown in [Table 16–1](#).

Table 16–1 Hosts in Each Topology

Topology	Hosts
OAM11g	IDMHOST1
	IDMHOST2
OAM10g/OIM11g	IDMHOST1
	IDMHOST2
	OAMHOST1
	OAMHOST2
	OIMHOST1
	OIMHOST2
OAM11g/OIM11g	IDMHOST1
	IDMHOST2
	OIMHOST1
	OIMHOST2

Table 16–1 (Cont.) Hosts in Each Topology

Topology	Hosts
OAAM11g	IDMHOST1
	IDMHOST2
	OAMHOST1
	OAMHOST2
OIF11g	IDMHOST1
	IDMHOST2
	OIFHOST1
	OIFHOST2

Note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware Home where Node Manager resides). See [Section 16.2, "Changing the Location of the Node Manager Log"](#) for further details.
2. Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See [Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"](#) for further details.

Note: The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

16.2 Changing the Location of the Node Manager Log

Edit the Node Manager properties file located at `MW_HOME/wlserver_10.3/common/nodemanager/nodemanager.properties`. Add the new location for the log file using the following line:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Oracle recommends that this location is outside the `MW_HOME` directory and inside the `admin` directory for the EDG.

Restart Node Manager, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) for the change to take effect.

16.3 Enabling Host Name Verification Certificates for Node Manager

Setting up host name verification certificates for communication between Node Manager and the administration server consists of the following steps:

- Step 1: [Generating Self-Signed Certificates Using the `utils.CertGen` Utility](#)
- Step 2: [Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility](#)
- Step 3: [Creating a Trust Keystore Using the `Keytool` Utility](#)
- Step 4: [Configuring Node Manager to Use the Custom Keystores](#)
- Step 5: [Configuring Managed WLS Servers to Use the Custom Keystores](#)
- Step 6: [Changing the Host Name Verification Setting for the Managed Servers](#)

16.3.1 Generating Self-Signed Certificates Using the `utils.CertGen` Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST.mycompany.com*) and a WLS 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 will need to 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 the steps below 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 examples below configure certificates for *HOST.mycompany.com* and *VIP.mycompany.com*; that is, it is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST.mycompany.com* is the address used by Node Manager and *VIP.mycompany.com* is the address used by a managed server or the administration server. This is the common situation for nodes hosting an administration server and a Fusion Middleware component, or for nodes where two managed servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the `WL_HOME/server/bin/setWLSEnv.sh` script. In the Bourne shell, run the following commands:

```
HOST> cd WL_HOME/server/bin
HOST> ./setWLSEnv.sh
```

Verify that the `CLASSPATH` environment variable is set:

```
HOST> echo $CLASSPATH
```

2. Create a user-defined directory for the certificates. For example, create a directory called 'certs' under the `ORACLE_BASE/admin/domain_name/aserver/domain_name` directory. Note that certificates can be shared across WLS domains.

```
HOST> cd ORACLE_BASE/admin/domain_name/aserver/domain_name
HOST> mkdir certs
```

Note: The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, etc.).

3. Change directory to the directory that you just created:

```
HOST> cd certs
```

4. Run the `utils.CertGen` tool from the user-defined directory to create the certificates for both `HOST.mycompany.com` and `VIP.mycompany.com`.

Syntax (all on a single line):

```
java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
[export | domestic] [Host_Name]
```

Examples:

```
HOST> java utils.CertGen welcome1 HOST.mycompany.com_cert
HOST.mycompany.com_key domestic HOST.mycompany.com
```

```
HOST> java utils.CertGen welcome1 VIP.mycompany.com_cert
VIP.mycompany.com_key domestic VIP.mycompany.com
```

16.3.2 Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility

Follow these steps to create an identity keystore on `HOST`:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, `ORACLE_BASE/admin/domain_name/aserver/domain_name/certs`).

Note: The identity store is created (if none exists) when you import a certificate and the corresponding key into the identity store using the `utils.ImportPrivateKey` utility.

2. Import the certificate and private key for both `HOST.mycompany.com` and `VIP.mycompany.com` into the identity store. Make sure 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:


```
HOST> java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity1 welcome1
ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/HOST.mycompany.com_
cert.pem
ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/HOST.mycompany.com_
key.pem
```

```
HOST> java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity2 welcome1
ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/VIP.mycompany.com_
cert.pem
ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/VIP.mycompany.com_
key.pem
```

16.3.3 Creating a Trust Keystore Using the Keytool Utility

Follow these steps to create the trust keystore on *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:

```
HOST> cp WL_HOME/server/lib/cacerts ORACLE_BASE/admin/domain_name/aserver/
domain_name/certs/appTrustKeyStore.jks
```

2. The default password for the standard Java keystore is 'changeit'. Oracle recommends always changing the default password. Use the keytool utility to do this. The syntax is:

```
HOST> keytool -storepasswd -new New_Password -keystore Trust_Keystore
-storepass Original_Password
```

For example:

```
HOST> keytool -storepasswd -new welcome1 -keystore appTrustKeyStore.jks
-storepass changeit
```

3. The CA certificate *CertGenCA.der* is used to sign all certificates generated by the *utils.CertGen* tool. It is located in the *WL_HOME/server/lib* directory. This CA certificate must be imported into the *appTrustKeyStore* using the keytool utility. The syntax is:

```
HOST> keytool -import -v -noprompt -trustcacerts -alias Alias_Name
-file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
HOST> keytool -import -v -noprompt -trustcacerts -alias clientCACert -file
WL_HOME/server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass
welcome1
```

16.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the *nodemanager.properties* file located in the *WL_HOME/common/nodemanager* directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
```

```

CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate

```

Make sure to use the correct value for `CustomIdentityAlias` on each node; that is, the custom identity alias specifically assigned to that node, for example for ...HOST2:

```

KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/aserver/domain_name/
certs/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity2
CustomIdentityPrivateKeyPassPhrase=welcome1

```

The passphrase entries in the `nodemanager.properties` file get encrypted when you start Node Manager as described in [Section 16.4, "Starting Node Manager."](#) For security reasons, you want to minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, you should start Node Manager as soon as possible so that the entries get encrypted.

When using a common/shared storage installation for `MW_HOME`, Node Manager is started from different nodes using the same base configuration (`nodemanager.properties`). In that case, it is required to add the certificate for all the nodes that share the binaries to the `appIdentityKeyStore.jks` identity store. To do this, create the certificate for the new node and import it to `appIdentityKeyStore.jks` as in [Section 16.3.2, "Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility."](#) Once the certificates are available in the store, each node manager needs to point to a different identity alias to send the correct certificate to the administration server. To do this, set different environment variables before starting Node Manager in the different nodes:

```

HOST> cd WL_HOME/server/bin
HOST> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX

```

Note: Make sure to specify the custom identity alias specifically assigned to each host, so 'appIdentity1' for ...HOST1 and 'appIdentity2' for ...HOST2.

16.3.5 Configuring Managed WLS Servers to Use the Custom Keystores

Follow these steps to configure the identity and trust keystores for `WLS_SERVER`:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Click the name of the server for which you want to configure the identity and trust keystores (`WLS_SERVER`). The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. In the Keystores field, select the "Custom Identity and Custom Trust" method for storing and managing private keys/digital certificate pairs and trusted CA certificates.
8. In the Identity section, define attributes for the identity keystore:

- **Custom Identity Keystore:** The fully qualified path to the identity keystore:
`ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/
appIdentityKeyStore.jks`
 - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in [Section 16.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#) This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order 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 or not you define this property depends on the requirements of the keystore.
9. In the Trust section, define properties for the trust keystore:
 - **Custom Trust Keystore:** The fully qualified path to the trust keystore:
`ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/
appTrustKeyStore.jks`
 - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in [Section 16.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#) This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order 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 or not 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.

In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in [Section 16.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."](#)
 15. Click **Save**.
 16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
 17. Restart the server for which the changes have been applied, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

16.3.6 Changing the Host Name Verification Setting for the Managed Servers

Once the steps above have been performed, you should set host name verification for the affected managed servers to `Bea Hostname Verifier`. To do this, perform the following steps:

1. Log in to Oracle WebLogic Server Administration Console.

2. Select **Lock and Edit** from the change center.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select the managed server in the Names column of the table. The settings page for the server is displayed.
6. Open the SSL tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `Bea Host Name Verifier`.
9. Click **Save**.
10. Click **Activate Changes**.

16.4 Starting Node Manager

Run these commands to start Node Manager on *HOST*:

Note: If you have not configured and started Node Manager for the first time yet, run the `setNMProps.sh` script as specified in [Section 16.4, "Starting Node Manager"](#) to enable the use of the start script for your managed servers.

```
HOST> cd WL_HOME/server/bin
HOST> ./startNodeManager.sh
```

Integrating Components

This chapter contains the following topics:

- [Section 17.1, "Migrating Policy and Credential Stores"](#)
- [Section 17.2, "Installing and Configuring WebGate"](#)
- [Section 17.3, "Integrating Administration Consoles with Single Sign-on 11g"](#)
- [Section 17.4, "Integrating Oracle Access Manager 10g and Oracle Identity Manager"](#)
- [Section 17.5, "Integrating Oracle Identity Manager and Oracle Access Manager 11g"](#)
- [Section 17.6, "Integrating Oracle Adaptive Access Manager with Oracle Access Manager"](#)
- [Section 17.7, "Integrating Oracle Adaptive Access Manager with Oracle Identity Manager"](#)
- [Section 17.8, "Integrating Oracle Identity Federation with Oracle Access Manager"](#)
- [Section 17.9, "Auditing Identity Management"](#)

17.1 Migrating Policy and Credential Stores

By default, policy store information is stored in a mixture of places, including the embedded LDAP directory and the file system. It is recommended that the policy store be placed into the external LDAP directory, so that:

- It is maintained in a central location
- It is included in the corporate centralized backup regime.

You begin policy and credential store migration by creating the JPS root and then you reassociate the policy and credential store with Oracle Internet Directory.

17.1.1 JPS Root Creation

On `OIDHOSTn`, create the `jpsroot` in Oracle Internet Directory using the command line `ldapadd` command as shown in these steps:

1. Create an `ldif` file similar to this:

```
dn: cn=jpsPolicy_edg
cn: jpsPolicy_edg
objectclass: top
objectclass: orclcontainer
```

2. Use `ORACLE_HOME/bin/ldapadd` to add these entries to Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f jps_root.ldif
```

17.1.2 Reassociating the Policy and Credential Store

To reassociate the policy and credential store with Oracle Internet Directory, use the `WLST reassociateSecurityStore` command. Follow these steps:

1. From `IDMHOST1`, start the `wlst` shell from the `ORACLE_COMMON_HOME/common/bin` directory. For example:

```
./wlst.sh
```

2. Connect to the WebLogic Administration Server using the `wlst connect` command shown below.

```
connect('AdminUser', "AdminUserPassword", t3://hostname:port')
```

For example:

```
connect("weblogic", "welcome1", "t3://idmhost-vip.mycompany.com:7001")
```

3. Run the `reassociateSecurityStore` command as shown below:

Syntax:

```
reassociateSecurityStore(domain="domainName", admin="cn=orcladmin",
password="orclPassword", ldapurl="ldap://LDAPHOST:LDAPPOR", servertime="OID",
jpsroot="cn=jpsRootContainer")
```

For example:

```
wls:/IDMDomain/serverConfig> reassociateSecurityStore(domain="IDMDomain",
admin="cn=orcladmin", password="password",
ldapurl="ldap://oid.mycompany.com:389", servertime="OID",
jpsroot="cn=jpsPolicy_edg")
```

The output for the command is shown below:

```
{servertime=OID, jpsroot=cn=jpsroot_idm, admin=cn=orcladmin,
domain=IDMDomain, ldapurl=ldap://oid.mycompany.com:389, password=password}
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)
```

```
Starting Policy Store reassociation.
LDAP server and ServiceConfigurator setup done.
```

```
Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Policy Store reassociation done.
Starting credential Store reassociation
LDAP server and ServiceConfigurator setup done.
Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
```

Credential Store reassociation done
Jps Configuration has been changed. Please restart the server.

4. Restart the Administration Server, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components,"](#) after the command completes successfully.

17.2 Installing and Configuring WebGate

Install and configure WebGate as follows.

17.2.1 Prerequisites

Ensure that the following tasks have been performed before installing the Oracle Web Gate:

1. Install and configure the Oracle Web Tier as described in [Chapter 5](#).
2. On Linux systems, make the special versions of the gcc libraries available, as described in [Chapter 17.2.1.1](#).

17.2.1.1 Making Special gcc Libraries Available

Oracle Web Gate requires special versions of gcc libraries to be installed (Linux only). These library files must exist somewhere on the Linux system. The Web Gate installer asks for the location of these library files at install time. These files are available from Oracle Technology Network at:

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

17.2.2 Creating WebGate Agents

Before installing WebGate into the web tier, a WebGate agent needs to be defined. This is achieved using either the remote registration agent, which is available on both IDMHOST1 and IDMHOST2 or the Oracle Access Manager Console. The following procedure should be followed to create the Web Gate agent.

- [Using the Remote Registration Utility](#)
- [Using Oracle Access Manager Administration Console](#)

17.2.2.1 Using the Remote Registration Utility

Use the remote registration utility as follows.

Creating an Agent Configuration File

The `oamreg.sh` script creates an agent configuration using the contents of a configuration file called `OAMRequest.xml`. You can find the template for this file in the directory `IAM_ORACLE_HOME/oam/server/rreg/input`.

Create a copy of this file on IDMHOST1, called `sso.xml`.

In the file supply details for the following attributes:

- **serverAddress:** URL of WebLogic Administration Server.
- **hostIdentifier:** IDMDomain
- **agentBaseUrl:** `https://sso.mycompany.com:443`

- **agentName:** Name used to identify the WebGate agent. Good practice is to use a name similar to `Webgate_myssso`.
- **autoCreatePolicy:** `False`
- **primaryCookieDomain:** Domain your servers reside in, for example: `.mycompany.com`
- **logOutUrls:** `/oamssso/logout.html`
- **security:** `open`

Here is a sample file:

```
<?xml version="1.0"?>
<!--
Copyright (c) 2009, 2010, Oracle and/or its affiliates. All rights reserved.

NAME: OAMRequest.xml - Template (with all options) for OAM Agent Registration
Request file
DESCRIPTION: Modify with specific values and pass file as input to the tool
-->
<OAMRegRequest>

    <serverAddress>http://ADMINHOSTVHN.mycompany.com:7001</serverAddress>
    <hostIdentifier>Webgate_myssso</hostIdentifier>
    <agentName>Webgate_myssso</agentName>
    <autoCreatePolicy>false</autoCreatePolicy>
    <primaryCookieDomain>.mycompany.com</primaryCookieDomain>
    <agentBaseUrl>https://sso.mycompany.com:443</agentBaseUrl>
    <maxCacheElems>100000</maxCacheElems>
    <cacheTimeout>1800</cacheTimeout>
    <cookieSessionTime>3600</cookieSessionTime>
    <maxConnections>1</maxConnections>
    <maxSessionTime>24</maxSessionTime>
    <idleSessionTimeout>3600</idleSessionTimeout>
    <failoverThreshold>1</failoverThreshold>
    <aaaTimeoutThreshold>-1</aaaTimeoutThreshold>
    <sleepFor>60</sleepFor>
    <debug>false</debug>
    <security>open</security>
    <denyOnNotProtected>0</denyOnNotProtected>
    <cachePragmaHeader>no-cache</cachePragmaHeader>
    <cacheControlHeader>no-cache</cacheControlHeader>
    <ipValidation>0</ipValidation>
    <logOutUrls>
        <url>/oamssso/logout.html</url>
    </logOutUrls>
    <protectedResourcesList>
        <resource>/sso.html</resource>
    </protectedResourcesList>
    <publicResourcesList>
        <resource>/public/index.html</resource>
    </publicResourcesList>
    <userDefinedParameters>
        <userDefinedParam>
            <name>MaxPostDataLength</name>
            <value>750000</value>
        </userDefinedParam>
        .....
        .....
    </userDefinedParameters>
```



```
</OAMRegRequest>
```

Creating Oracle Access Manager Agent

The agent configuration is created by running the `oamreg.sh` script. This is done by issuing the following commands from within the `RREG_HOME` directory:

```
export JAVA_HOME=$MW_HOME/jrockit_160_14_R27.6.5-32
./bin/oamreg.sh inband input/sso.xml
```

When the script runs you will be asked for the following information. Provide the values shown:

```
Agent User Name: oamadmin
Agent Password: oamadmin user's password
Do you want to enter a Web Gate Password: y
Enter password for webgate and confirm
```

Note: Although it is not mandatory to provide a password for Web Gate, Oracle highly recommends that you do so. It is mandatory when wiring Oracle Identity Management to Oracle Access Manager.

This will then create a file called `ObAccessClient.xml` in the directory `RREG_HOME/output/Agent_Name`.

Copy this file to each webgate installation. Put it in the directory: `WEBGATE_INSTALL_DIR/access/oblix/lib`.

17.2.2.2 Using Oracle Access Manager Administration Console

Access the Oracle Access Manager console at:

```
http://admin.mycompany.com:7001/oamconsole
```

Log in as the `oamadmin` user.

Click **Add OAM 10g Agent**.

Complete the following information:

- **Agent Name:** Name for this Agent, for example: `Webgate_mysso`
- **Access Client Password:** Enter a Password for Web Gate to use

Note: Although it is not mandatory to provide a password for Web Gate, Oracle highly recommends that you do so. It is mandatory when wiring Oracle Identity Management to Oracle Access Manager.

- **Agent Base URL:** `http://sso.mycompany.com:443`
- **Host Identifier:** `IDMDomain`
- Ensure that Auto Create Policies is *not* selected.
- **Protected Resources:** enter protected resources, as required

Note: To make testing easier, it is useful to create a simple HTML file called `sso.html` in `ORACLE_INSTANCE/config/OHS/ohs1/htdocs`.

Choose to protect `/sso.html`. This will enable you to verify that SSO is working by accessing the URL:
`https://mysso.us.oracle.com/sso.html`.

Click **Apply**.

This will then create a file called `ObAccessClient.xml` in the directory `DOMAIN_HOME/output/Agent Name`.

Copy this file to each webgate installation. Place it in the directory: `WEBGATE_INSTALL_DIR/access/oblix/lib`.

17.2.2.3 Update Newly-Created Agent

After generating the initial configuration, you must edit the configuration and add advanced configuration entries.

1. Select **System Configuration** Tab
2. Select **Agents - OAM Agents - version Agents** from the directory tree.
3. Click the newly created agent (`Webgate_mysso`).
4. Select **Open** from the Actions Menu.
5. Verify that all of your access servers are listed in the Primary Servers List box. If any are missing, click the **Add** icon (+) to add a new preferred server.
6. If any access servers are missing add them to the Primary or Secondary Server list.
7. Update the following information:
 - **Primary cookie domain:** `.mycompany.com` (include the dot at the beginning).
 - **Logout URL:** `/oamssso/logout.html`
8. Click **Apply**.

17.2.3 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before you install Oracle Webgate, ensure that the managed servers `WLS_OAM1` and `WLS_OAM2` are started.

Install Oracle WebGate as described in the following sections.

17.2.3.1 Oracle WebGate 10g

Start the Web Gate installer by issuing the command:

```
Oracle_Access_Managerversion_linux_OHS11g_WebGate -gui
```

Then perform the following steps:

1. On the Welcome to the InstallShield Wizard for Oracle Access Manager WebGate screen.
Click **Next**.

2. On the Customer Information screen, enter the username and group that the Identity Server will use. The default value for username and group is nobody. For example, enter `oracle/oinstall`.

Click **Next**.

3. On the installation type screen enter **Install and configure**.
4. Specify the installation directory for Oracle Access Manager Access Server. For example, enter: `MW_HOME/oam/webgate`.

Click **Next**.

Note: Oracle Access Manager WebGate is installed in the `access` subdirectory under `/u01/app/oracle/product/fmw/oam/webgate`.

5. Oracle Access Manager WebGate will be installed in:
`/u01/app/oracle/product/fmw/oam/webgate/`

The access directory is created by the installer automatically.

6. Specify the location of the GCC run-time libraries, for example:
`/u01/app/oracle/oam_lib`

Click **Next**.

7. The installation progress screen is shown. After the installation process completes, the WebGate Configuration screen appears.

8. On the WebGate Configuration screen, you are prompted for the transport security mode:

The transport security between all Access System components (Policy Manager, Access Servers, and associated WebGates) must match; select one of the following: Open Mode, Simple Mode, or Cert Mode.

Select **Open Mode**.

Click **Next**.

9. On the next WebGate Configuration screen, specify the following WebGate details:

- **WebGate ID:** The agent name used in [Section 17.2.2.2, "Using Oracle Access Manager Administration Console,"](#) for example `Webgate_mysso`.
- **Password for Web Gate:** If you entered a password when creating the agent, enter this here. Otherwise leave blank.
- **Access Server ID:** `WLS_OAM1`
- **Host Name:** Enter the Host name for one of the access servers for example `IDMHOST1`
- **Port Number the Access Server listens to:** *ProxyPort*

Note: To find the port that the Access Server is using, log into the oamconsole using the URL:

`http://admin.mycompany.com:7001/oamconsole`. Then perform the following steps:

1. Select the **System Configuration** tab.
2. Select **Server Instances**.
3. Select Instance (`WLS_OAM1`) and click the **View** icon in the tool bar.

The proxy entry will have host and port information.

10. On the Configure Web Server screen, click **Yes** to automatically update the web server, then click **Next**.
11. On the next Configure Web Server page, a message informs you that the Web Server configuration has been modified for WebGate.
Click **Next**.
12. Stop and start your Web server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) to enable configuration updates to take effect.
Click **Next**.
13. The next screen, Configure Web Server, displays the following message:

```
If the web server is setup in SSL mode, then httpd.conf file needs to be configured with the SSL related parameters. To manually tune your SSL configuration, please follow the instructions that come up.
```


Click **Next**.
14. The next screen, Configure Web Server, displays a message with the location of the document that has information on the rest of the product setup, as well as Web Server configuration.
Select **No** and click **Next**.
15. The final Configure Web Server screen appears with a message to manually launch a browser and open the HTML document for further information on configuring your Web Server.
Click **Next**.
16. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next**.
17. A message appears, along with the details of the installation, informing you that the installation was successful.
Click **Finish**.
18. Replace the file `ObAccessClient.xml` in the directory `MW_HOME/webgate/access/oblix/lib/` with the file generated in [Section 17.2.2.2, "Using Oracle Access Manager Administration Console."](#)
19. Restart the web server by following the instructions in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
20. Repeat for `WEBHOST2`

17.2.4 Validating WebGate

Assuming that you created a protected resource called `sso.html` in [Section 11.9, "Validating Oracle Access Manager,"](#) you can test that webgate is functioning by accessing the URL:

```
https://sso.mycompany.com:443/sso.html
```

You are prompted to log in to Oracle Access Server. Once you have done so, the Oracle FMW home page is displayed.

Note: At this point, if you attempt to access consoles such as WebLogic, OAM, or OIM, you will have to log on twice. This is because WebGate protects these resources. For this reason, you should perform the steps in [Section 17.3, "Integrating Administration Consoles with Single Sign-on 11g"](#) next.

17.3 Integrating Administration Consoles with Single Sign-on 11g

This section describes how to integrate administration consoles with single sign-on.

Note: Once you have enabled single sign-on for the administration consoles, ensure that at least one OAM server is running in order to enable console access.

If you have used the Oracle Weblogic console to shut down all of the OAM managed servers, then restart one of those managed servers manually before using the console again.

To start WLS_OAM1 manually, use the command:

```
DOMAIN_HOME/bin/startManagedWeblogic.sh WLS_OAM1 t3://ADMINVHN:7001
```

17.3.1 Prerequisites

Before you attempt to integrate administration consoles with single sign-on, ensure that the following tasks have been performed:

1. Configure Oracle HTTP Server, as described in [Chapter 5](#).
2. Configure Oracle Identity Manager, as described in [Chapter 13](#).
3. Install and Configure WebGate, as described in [Section 17.2](#).

17.3.2 Creating Oracle Virtual Directory Authenticator

1. Log in to the WebLogic Administration Console at `http://admin.mycompany.com/console`.
2. Click **Security Realms** from the Domain structure menu.
3. Click **Lock and Edit** in the Change Center.
4. Click **myrealm**.
5. Select the **Providers** tab.
6. Click **DefaultAuthenticator**.
7. Set **Control Flag** to **SUFFICIENT**.

8. Click **Save**.
9. Click **Security Realms** from the Domain structure menu.
10. Click **myrealm**.
11. Select the **Providers** tab.
12. Click **New**.
13. Supply the following information:
 - **Name:** OVDAuthenticator
 - **Type:** OracleVirtualDirectoryAuthenticator
14. Click **OK**.
15. Click **Reorder**.
16. Click **OVDAuthenticator**.
17. Using the arrows on the right hand side, position **OVDAuthenticator** so that it is second in the list.
18. Click **OK**.
19. Click **OVDAuthenticator**.
20. Set **Control Flag** to **SUFFICIENT**.
21. Click **Save**.
22. Select the **Provider Specific** tab.
23. Enter the following details:
 - **Host:** ovd.mycompany.com
 - **Port:** 389
 - **Principal:** cn=orcladmin
 - **Credential:** orcladmin password
 - **Confirm Credential:** orcladmin password
 - **User Base DN:** cn=Users,dc=mycompany,dc=com
 - **Group Base DN:** cn=Groups,dc=mycompany,dc=com
 - **GUID Attribute:** orclguid
24. Click **Save**.
25. Restart the Administration Server and all the managed servers, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

Validating the Configuration

Validate the configuration by logging in to the oamconsole as the user oamadmin.

You can perform a further validation test by using the Oracle WebLogic Administration Console, as follows.

1. Log in to the console, which is at <http://admin.mycompany.com/console>.
2. Select **Security Realms** from the Domain structure menu.
3. Click **myrealm**.
4. Click the **Users and Groups** tab.

5. Click **Users**.
LDAP users will be displayed.

17.3.3 Creating Oracle Access Manager Identity Asserter

1. Log in to the WebLogic Administration Console at:
`http://admin.mycompany.com:7001/console`.
2. Click **Security Realms** from the Domain structure menu.
3. Click **Lock and Edit** in the **Change Center**.
4. Click **myrealm**.
5. Select the **Providers** tab.
6. Click **New**.
7. Supply the following information:
 - **Name:** OAMIdentityAsserter
 - **Type:** OAMIdentityAsserter
8. Click **OK**.
9. Click **Reorder**.
10. Click **OAMIdentityAsserter**.
11. Using the arrows on the right hand side, position **OAMIdentityAsserter** so that it is first in the list.
12. Click **OK**.
13. Click **OAMIdentityAsserter**.
14. Set **Control Flag** to **REQUIRED**.
15. Click **Save**.
16. Click **Activate Changes**.

17.4 Integrating Oracle Access Manager 10g and Oracle Identity Manager

This section describes how to integrate Oracle Access Manager and Oracle Identity Manager.

17.4.1 Prerequisites

Ensure that the following tasks have been performed before integrating OAM 10 with OIM 11g.

1. Set the `oamEnabled` flag for the Change Log and User Adapters in OVD by using the ODSM console.
2. Update the LDAP schema definitions and ACL's with the OAM and OIM password Expiry schema extensions, as described in [Section 17.4.1.1](#).
3. Create a user in OIM with System Administrator privileges by using the Oracle Identity Manager Administration Console. This user will be used for Administrative tasks in OAM and OIM.
4. Patch Access Sever to enable support for the OAM and OIM integration, as described in [Section 17.4.1.2](#)

17.4.1.1 Update the LDAP Schema Definitions

Update the LDAP Schema Definitions and ACLs with the OAM and OIM password expiry schema extensions, as follows:

1. Create an LDIF file called `PasswordExpired.ldif` with the following contents:

```
dn: cn=subSchemaSubEntry
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.3831.0.0.400 NAME 'obpasswordexpirydate' DESC
'Oracle Access Manager defined attribute type' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' X-ORIGIN 'user defined' )

dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.3831.0.1.40 NAME 'OIMPersonPwdPolicy' DESC 'Oracle
Access Manager defined objectclass' SUP top AUXILIARY MAY (
obpasswordexpirydate ) )
```

2. Update the LDAP schema by using the `ldapadd` command.

17.4.1.2 Patching the Access Server

Follow these steps to patch the Access Server:

1. Locate the OAM access server patch package. The patch name is `Oracle_Access_Manager10_1_4_3_0_BP01_Patch_linux_Access_Server.zip`
2. Shut down Oracle Access Manager 10.1.4.3.0.
3. Unzip the `Oracle_Access_Manager10_1_4_3_0_BP01_Patch_linux_Access_Server.zip` to a temporary location
4. Change directory to `PatchExtractLocation/Oracle_Access_Manager10_1_4_3_0_BP01_Patch_linux_Access_Server_binary_parameter`.
5. Start the patch installation tool as:

```
./patchint -i InstallDir/access
```

where *InstallDir* is the path to the Access Server install location.

This applies the BPFA patch for OAM-OIM integration to the OAM 10.1.4.3.0 Access Server.

6. Start the access server
7. Start the other Oracle Access Manager components.

17.4.2 Creating Policies in Oracle Access Manager 10g

To protect OIM pages from unauthorized access, OAM needs to be configured to protect these pages. OAM Access Server requires that OAM Policies be defined to specify which OIM pages need to be protected and authentication mechanism to be used for authenticating users.

Run the OAM Config Tool on `OAMADMINHOST` as follows to configure the OAM policy to protect OIM pages. This single step using OAM Config Tool configures OAM Policy to protect OIM page and configures OAM password policy to integrate with the OAM login pages for Fusions Applications and with OIM password management.

```
[Prompt> java -jar oamcfgtool.jar mode=CREATE app_domain=Policy_Domain_Name web_
```



```

domain=Host_Identifier uris_file=Policy_Configuration_File ldap_host=LDAP_Host
ldap_port=LDAP_Port ldap_userdn=LDAP_Bind_User_DN ldap_userpassword=LDAP_Bind_
User_Password oam_aaa_host=Access_Server_Host oam_aaa_port=Access_Server_Port oam_
aaa_mode={OPEN | SIMPLE | CERT} oam_aaa_passphrase=Global_Pass_Phrase
-usei18nlogin authenticating_wg_url=http://awghost.domain:port
-configOIMPwdPolicy OimOhsHostPort=http://OimHost:Port
Jul 12, 2010 4:08:53 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Processed input parameters
Jul 12, 2010 4:08:53 PM oracle.security.oam.oamcfg.OAMCfgTool
getVarsFromOverrideMap
WARNING: OAMCFG-60066: An unexpected parameter has been passed to the tool,
OimOhsHostPort
Jul 12, 2010 4:08:53 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Initialized Global Configuration
Jul 12, 2010 4:09:06 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Successfully completed the Create operation.
Jul 12, 2010 4:09:06 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Operation Summary:
Jul 12, 2010 4:09:06 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Policy Domain : IDMEDG1
Jul 12, 2010 4:09:06 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Host Identifier: IDMEDG1
Jul 12, 2010 4:09:06 PM oracle.security.oam.oamcfg.OAMCfgTool main
INFO: Access Gate ID : IDMEDG1_AG

```

Note that the `oim.oam.conf` file contains public and protected URIs of OIM. You can add any URI depending on the apps you are using. This section contains an example of the `oim_oam.conf` file.

web_domain: You have created and configured a Host Identifier while creating WebGate entries. The same host identifier should be specified as `web_domain` when running the OAM Configuration Tool.

usei18nlogin: This parameter indicates that Internationalized Login Pages should be used for protecting OIM pages as configured in `oim.oam.conf` file.

Default values would be used for the below three password policy related parameters in OAM with the value in `OimOhsHostPort` pre-pended to these. For example:

```

OimLostPwdRedirectUrl (Lost Password Redirect URL):
  <OimOHSHostPort>/admin/faces/pages/forgotpwd.jspx
OimPwdRedirectUrl (Password Change Redirect URL):
  <OimOHSHostPort>/admin/faces/pages/pwdmgmt.jspx?backUrl=%RESOURCE%
OimLockoutRedirectUrl (Account Lockout Redirect URL):
  <OimOHSHostPort>/ApplicationLockoutURI

```

This will create the following:

- Policy Domain to protect OIM Pages from unauthenticated access. Also adds specific policies to allow anonymous access to common JavaScripts / CSS / image files and to OIM pages responsible for providing Forgot Password, Self Registration and Track Registration functionality.
- Authentication Schemes to be used while protecting OIM Pages using OAM Policies.
- Password Policy required in OAM Identity System Console to enable OAM Access Server to redirect users to OIM Password Management pages for Force Password Reset.
- Password Policy Redirect URLs in OAM Identity System Console to specify OIM URLs for Forgot Password, Change on Password Reset and Account Lockout.

17.4.3 Enabling Oracle Access Manager 10g and Oracle Identity Manager Integration

- Navigate to `Access_Server_installDir/access/oblix/apps/common/bin`. Edit `globalparams.xml` file and add following block in file.

```
* <SimpleList>
    <NameValPair
        ParamName="OIMIntegration"
        Value="true"></NameValPair>
</SimpleList>
```

- Save the file and restart the Access Server, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
- Also restart Identity Server. (This is required if you are using the OAM Config Tool to create and configure Password Policies)
- Go to **Access System Console > Access System Configuration > Authentication Management > OraDefaultI18NFormAuthNScheme**. You will see the I18N Form Authentication Scheme created as shown below.

Click **Modify** and set Authentication Level for this scheme to 5. Also add `OIMStepDownAuthLevel:1` as Challenge Parameter as shown below,

You must configure WebGate Login Pages for proper functioning of Form based Authentication with Internationalization Support.

- To enable Register and Track Registration links, you need to set `hideRegLink` variable in `config.js` to false (located under `WebGate/access/oamssso/global` on `webhost1` and `webhost2`). Also set value for `OimOHSHostPort` variable to the host and port of OHS instance front ending your OIM instance. See below:

Ensure that, Lost Password (var `lostPasswordURL`), Register (var `registrationURL`) and Track Reregistration (var `trackRegistrationURL`) links in `config.js` are pointing to correct OIM URLs, which are

```
/admin/faces/pages/forgotpwd.jspx,
/oim/faces/pages/Uself.jspx?OP_TYPE=SELF_REGISTRATION&T_ID=Self-Register%20User&E_TYPE=USELF, and
/oim/faces/pages/Uself.jspx?E_TYPE=USELF&OP_TYPE=UNAUTH_TRACK_REQUEST respectively.
```

- Logout Processing 1: Update `defaultAWGEndURL`, `defaultendURL`, and `mapAgentIdToAgentHostPort` variables in `config.pl` (under `cgi-bin` of OHS11g instance) to reflect correct values for your deployment. `defaultAWGEndURL`, `defaultendURL` are used as `end_url` in case none is specified in the query-string while invoking logout. `mapAgentIdToAgentHostPort` is used to map WebGate IDs in your deployment to their respective WebServer host-port. These values are crucial for correct functioning of Logout.
- Logout Processing 2: You must update all WebGate entries except for the Authentication WebGate and add User Defined Parameter, `logoutRedirectUrl` with value as `http://admin.mycompany.com:80/cgi-bin/logout.pl`. For this, navigate to each of Resource WebGate entry (except for the Authentication WebGate) and click **Modify**. Specify `logoutRedirectURL` as a User Defined Parameter with proper values and Save the profile.

17.4.4 Configuring Oracle Access Manager 10g/Oracle Identity Manager Authenticator

1. Start Administration Server
2. Go to the WebLogic Administration Console at `http://WL_HOST:WL_PORT/console`.
3. Configuring Authentication
 - Click **Security Realms > myrealm > Providers**.
 - Create a new Provider of type OAM Identity Asserter
 - Mark the control flag as **REQUIRED**
 - Reorder to move this provider at the first place
4. OIM Authenticator
 - Mark **Default Authenticator** as **SUFFICIENT** and move it to second place
 - Mark **OIM Authenticator** as **OPTIONAL** and reorder to move OIM Authenticator in 3rd place.
5. OID Authenticator
 - Create a new provider of type OracleInternetDirectory Authenticator
 - In Provider Specific tab, Fill up the LDAP details (The LDAP used by OAM)
 - Mark it as SUFFICIENT and place it fourth
6. Make Authentication Providers order as below. OAM ID asserter should be on top and so on.

17.4.5 Configuring Auto-Login for Oracle Identity Manager

1. Update the MDS Schema with OAM Information

Update oim-config.xml

```
<ssoConfig>
  <version>@oamVersion</version>
  <accessServerHost>@oamAccessServerHost</accessServerHost>
  <accessServerPort>@oamAccessServerPort</accessServerPort>
  <accessGateID>@oamAccessGateID</accessGateID>
  <cookieDomain>@oamcookieDomain</cookieDomain>
  <napVersion>1</napVersion>
  <transferMode>OPEN</transferMode>
  <webgateType>ohsWebgate10g</webgateType>
  <ssoEnabled>>false</ssoEnabled>
</ssoConfig>
```

For example, make the changes in oim-config.xml like this:

```
<ssoConfig>
  <version>10.1.4.3</version>
  <accessServerHost>dadvm10203.us.oracle.com</accessServerHost>
  <accessServerPort>7044</accessServerPort>
  <accessGateID>OAM_AG</accessGateID>
  <napVersion>3</napVersion>

  <cookieDomain>.us.oracle.com</cookieDomain>
  <transferMode>open</transferMode>
  <ssoEnabled>>true</ssoEnabled>
```

```
</ssoConfig>
```

REFERENCE: Updating Files Located in MDS

- a. Set OIM_ORACLE_HOME to ORACLE_HOME
- b. Go to *ORACLE_HOME*/server/bin
- c. Edit *weblogic.properties*

```
wls_oim1          = Server name OIM (Its oim_server1 by default in shiphome)
application_name  = OIMMetadata
metadata_from_loc = make a new folder (Say /tmp/mds_from)
metadata_to_loc   = make a new folder (say /tmp/mds_to)
metadata_files    = /db/oim-config.xml
```

- d. Run *weblogicExportMetadata.sh*. This will export the file to */tmp/mds_to*
 - e. Update and copy to */tmp/mds_from* and Run *weblogicImportMetadata.sh*. This will import the updated file
2. Seed Access Gate Password in CSF.

Note: The steps shown here are for Open security mode. If the security mode is set to Simple, configure the keystore as described in *Oracle Access Manager Access Administration Guide* in the Oracle Access Manager 10g (10.1.4.3) Documentation Library

Seed Access gate password in CSF against Map name *oim* and key name *SSOAccessKey*. This CSF is present at *DOMAIN_HOME/config/fmwconfig* by name *cwallet.sso*

Run *ORACLE_HOME/common/bin/wlst.sh*

```
connect()
createCred(map="oim",
key="SSOAccessKey", user="SSOAccessKey", password="welcome1", desc="OAMAccessGateP
assword")
listCred(map="oim", key="SSOAccessKey")
```

3. Enable WLS Plug-ins

Go to WebLogic Administration console for OIM. Click **Environment > servers > wls_oim1 > Advanced**

Select **WebLogic Plug-In Enabled** if not selected already.

4. Import SSO Notification Eventhandlers in OIM

Import following event handler: *ORACLE_HOME/server/oamMetadata/db/ssointg/EventHandlers.xml*

Copy *ORACLE_HOME/server/oamMetadata/db/ssointg/EventHandlers.xml* to some temporary location, for example:
/tmp/mds/db/ssointg/EventHandlers.xml.

Update *weblogic.properties* with *metadata_from_loc=/tmp/mds* and *file_names=/db/ssointg/EventHandlers.xml*

Update other property names.

Run:

```
"sh weblogicImportMetadata.sh"
```

- Restart the Servers, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

17.5 Integrating Oracle Identity Manager and Oracle Access Manager 11g

This section describes how to integrate Oracle Identity Manager and Oracle Access Manager 11g.

17.5.1 Prerequisites

17.5.2 Updating Single Sign-on Provider Configuration

Update the single sign-on provider configuration using the `wlst addOAMSSOProvider` command. This command configures the Oracle Access Manager JPS SSO Service Provider. It modifies domain level `jps-config.xml` file to add an OAM SSO service instance and required properties. The syntax for the command is:

```
addOAMSSOProvider(loginuri="login_uri", logouturi="logout_uri",
autologinuri="autologin_uri")
```

where:

- `loginuri` is the login URI that triggers SSO authentication. This is a required parameter.
- `logouturi` is the logout URI that logs out the signed-on user. This is an Optional parameter.
- `autologinuri` is the auto login URI. This is an optional parameter.

Note: This command must be executed in online mode only, that is, when the Administration Server is running.

Follow these steps to configure Oracle Access Manager for Oracle Identity Manager integration.

- Run `wlst.sh` from the `ORACLE_HOME/common/bin` directory to invoke the WLST shell.
- Connect to the WebLogic Administration Server using the `connect` command
- Run the `addOAMSSOProvider` WLST command to configure the Oracle Access Manager JPS SSO Service Provider.

For example:

```
Prompt> ./wlst.sh
wls:/offline>connect('weblogic',password,'t3://idmhost1-vip.mycompany.com:7001')
)
```

```
wls:/IDMDomain/serverConfig>
```

```
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",logouturi="/oams
```

```
so/logout.html", autologinuri="/obrar.cgi")
```

17.5.3 Configure Oracle Access Manager for Oracle Identity Manager Integration

Update the configuration for the Oracle Access Manager managed servers using the `wlst updateOIMHostPort` command. This command updates the `IdentityManagement`, `ServerConfiguration` sections of the `oam-config.xml` file with host and port details for Oracle Identity Manager. The syntax for the command is:

```
updateOIMHostPort(hostName = "host_name", port = "port_number", secureProtocol = "[ true | false ]")
```

where:

- `hostname` is the Load Balancer VIP configured to route traffic to the OIM Managed Servers in this enterprise topology. This is a required parameter. For example: `https://sso.mycompany.com`.
- `port` is the listen port for the load balancer. This is a required parameter.
- `secureProtocol`: specifies whether or not the communication protocol is secure. This is a required parameter. Set this to `Yes` when using `https` and `No` when using `http`. Please note that

Note: This command must be executed in online mode only, that is, when the Administration Server is running.

Follow these steps to configure Oracle Access Manager for Oracle Identity Manager integration.

1. Run the `wlst.sh` script under `ORACLE_HOME/common/bin` to invoke the WLST shell.
2. Connect to the WebLogic Administration Server using the `connect` command.
3. Run the `updateOIMHostPort()` WLST command to update the OAM configuration.

For example:

```
Prompt> ./wlst.sh
wls:/offline>
connect('weblogic', password, 't3://idmhost1-vip.mycompany.com:7001')
wls:/IDMDomain/serverConfig> updateOIMHostPort(hostName = "sso.mycompany.com" ,
port = "443", secureProtocol = "true")
```

4. Validate that the command completed successfully by checking the `IdentityManagement`, `ServerConfiguration` sections of the `oam-config.xml` file under the `DOMAIN_HOME/config/fmwconfig` directory. The `IdentityManagement`, `ServerConfiguration` should look similar to this snippet:

```
<Setting Name="IdentityManagement" Type="htf:map">
  <Setting Name="ServerConfiguration" Type="htf:map">
    <Setting Name="OIM-SERVER-1" Type="htf:map">
      <Setting Name="Host"
Type="xsd:string">sso.mycompany.oracle.com</Setting>
      <Setting Name="Port" Type="xsd:integer">443</Setting>
      <Setting Name="SecureMode" Type="xsd:boolean">True</Setting>
```

```
</Setting>
</Setting>
```

17.5.4 Integrating Oracle Access Manager with Oracle Identity Manager using the OIM Configuration Tool

Use the OIM Configuration tool, `oimcfgtool.jar`, under the `IAM_ORACLE_HOME/server/ssointg` directory to wire OAM with OIM on all the hosts. For complete information about the tool, see "Configuring the Authentication Scheme for the Identity Asserter" in *Oracle Fusion Middleware Application Security Guide*.

17.5.4.1 Prerequisites

Ensure that the following criteria have been met before running `oimcfgtool`:

1. The `wlfullclient.jar` file exists under the `MW_HOME/wlserver_10.3/server/lib` directory. If the jar file not present, generate the jar file by following the steps in [Section 13.5, "Post-Installation Steps on OIMHOST1 and OIMHOST2."](#)
2. You are running `oimcfgtool` from the `IAM_ORACLE_HOME/server/ssointg` directory. Do not copy this tool to a different location.
3. The Sun JDK is available in the `PATH`.

17.5.4.2 Using OIM Configuration Tool

Follow these steps to integrate OAM with OIM using `oimcfgtool`.

Notes:

- Ensure that the OIM and SOA Managed Servers are up and running before you run `OIMCFGTOOL`.
 - Do not restart any of the servers until all the steps in this section are completed.
-
-

1. Set your `ORACLE_HOME` to the `IAM_ORACLE_HOME`, the `JAVA_HOME` to the `JDK6` directory and make sure that `PATH` includes `JAVA_HOME`.

```
prompt>export MW_HOME=/opt/maa/oracle/plus/product/fmw
prompt>export ORACLE_HOME=/opt/maa/oracle/plus/product/fmw/iam
prompt>export JAVA_HOME=/opt/maa/oracle/plus/product/fmw/jdk160_18
prompt>export PATH=$JAVA_HOME/bin:$PATH
```

2. Run the `oimcfgtool` with the `generate-profile` option to create the `sso-config.profile` file. Provide your inputs in `sso-config.profile`. You will be prompted for required inputs not provided in profile file. Run the tool as follows:

```
java -jar oimcfgtool.jar generate-profile
```

The output is similar to this:

```
java -jar oimcfgtool.jar generate-profile
Turning off debug logs
```

```
Generating sso-config.profile...
```

Generated sso-config.profile

3. Edit the `sso-config.profile` file created under `IAM_ORACLE_HOME/server/ssointg` directory. Provide the values as shown:

```
Access Server Host :-sso.mycompany.com
Access Server Port :-443
Access Gate ID :-IDMEDGAccessGate1
Cookie Domain :-.mycompany.com
Cookie Expiry Interval :-120
OAM Transfer Mode OPEN/SIMPLE/CERT :-OPEN
Webgate type javaWebgate/ohsWebgate10g/ohsWebgate11g :-ohsWebgate10g
SSO Enabled Flag :-true
MDS DB Url :-jdbc:oracle:thin:@oimdb1-vip.us.oracle.com:1521:oimdb1
MDS DB Schema Username :-J12_MDS
Domain Location :-/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain
WLS Server URL :-t3://ADMINHOSTVHN.mycompany.com:7001
WLS Username :-weblogic
Domain Name :-IDMDomain
OIM Managed Server Name :-wls_oim1
LDAP Host :-oid.mycompany.com
LDAP Port :-389
LDAP Root DN :-cn=orcladmin
User Search Base :-cn=Users,dc=mycompany,dc=com
Group Search Base :-cn=Groups,dc=mycompany,dc=com
Password Expiry Period in Days :-7300
```

4. Run `oimcfgtool` with the option to update the access server information in the `oim-config.xml` file. Run the tool as follows:

```
java -jar oimcfgtool.jar update-oim-config
```

The output will be similar to this:

```
java -jar oimcfgtool.jar update-oim-config
Turning off debug logs
***** Seeding OAM Config in OIM *****
Loading inputs from sso-config.profile
Completed loading inputs from sso-config.profile
Remaining inputs will be queried from console.
Completed loading user inputs for - OAM Access Config
Enter MDS DB Schema Password:
Completed loading user inputs for - MDS DB Config
Validated input values
Initialized MDS resources

Jun 25, 2010 1:30:50 PM oracle.mds
NOTIFICATION: transfer operation started.
Jun 25, 2010 1:30:51 PM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
Download from DB completed
Releasing all resources
Updated oamMetadata/db/oim-config.xml
Initialized MDS resources

Jun 25, 2010 1:30:51 PM oracle.mds
NOTIFICATION: transfer operation started.
Jun 25, 2010 1:30:53 PM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
```



```
Upload to DB completed
```

```
Releasing all resources
OAM configuration seeded. Please restart oim server.
*****
Operation completed. Please restart all servers.
```

5. Run the `oimcfgtool` with the `seed-oam-passwords` option to seed the OAM webgate passwords in the Credential Store. Run the tool as follows:

```
java -jar oimcfgtool.jar seed-oam-passwords
```

The output is similar to this:

```
java -jar oimcfgtool.jar seed-oam-passwords
Turning off debug logs
***** Seeding OAM Passwds in OIM *****
Loading inputs from sso-config.profile
Completed loading inputs from sso-config.profile
Remaining inputs will be queried from console.

Enter SSO Access Gate Password:
Enter ssoKeystore.jks Password:
Enter SSO Global Passphrase:

Completed loading user inputs for - CSF Config
Updating CSF with Access Gate Password...
Updating CSF ssoKeystore.jks Password...
Updating CSF for SSO Global Passphrase Password...
*****
Operation completed. Please restart all servers.
```

6. Run the `oimcfgtool` with the `seed-oam-metadata` option to upload the OAM notification handlers. Run the tool as follows:

```
java -jar oimcfgtool.jar seed-oam-metadata
```

The output will be similar to this:

```
java -jar oimcfgtool.jar seed-oam-metadata
Turning off debug logs
***** Activating OAM Notifications *****
Loading inputs from sso-config.profile
Completed loading inputs from sso-config.profile
Remaining inputs will be queried from console.
Enter MDS DB Schema Password:

Completed loading user inputs for - MDS DB Config
Initialized MDS resources
Jun 25, 2010 1:40:58 PM oracle.mds
NOTIFICATION: transfer operation started.
Jun 25, 2010 1:40:59 PM oracle.mds
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
Upload to DB completed
Releasing all resources
Notifications activated.
*****
Operation completed. Please restart all servers.
```

7. Proceed as follows

- a. Create the Oracle Virtual Directory Authenticator as described in [Section 17.3.2, "Creating Oracle Virtual Directory Authenticator."](#)
- b. Create the Oracle Access Manager Identity Asserter described in [Section 17.3.3, "Creating Oracle Access Manager Identity Asserter."](#)
- c. Reorder the Authenticators as follows:
 - OAM Identity Asserter REQUIRED**
 - Default Authenticator SUFFICIENT**
 - OIM Signature Authenticator SUFFICIENT**
 - OVD Authenticator SUFFICIENT**
 - OIM Authentication Provider OPTIONAL**
8. Stop and Start the WLS Admin Server and all the Managed Servers in the domain as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

17.5.5 Seed the xelsysadm User in Oracle Internet Directory

You must create the xelsysadm user manually in Oracle Internet Directory. Follow the steps below to create this user

1. Create a file called xelsysadm.ldif with the following contents:

```
dn: uid=xelsysadm,dc=mycompany,dc=com
obpasswordchangeflag: false
obpasswordexpirydate: 2035-01-01T00:00:00Z
sn: admin
uid: xelsysadm
givenname: xelsysadm
displayname: xelsysadm
cn: xelsysadm
objectclass: orclIDXPerson
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
userpassword: <xelsysadm password>
orclisenabled: ENABLED
```

2. Use the ldapadd command seed the xelsysadm in LDAP. Run the ldapadd command against OVD to create the user.

```
ldapadd -h ovd.mycompany.com -p 389 -D cn="orcladmin" -q -f xelsysadm.ldif
```

17.5.6 Updating Oracle Identity Manager Configuration

Update the Oracle Identity Manager configuration with the Webgate Agent Type. This value must be updated in the oim-config.xml file.

Execute these steps on IDMHOST1, the host where the administration server is running:

1. Use the OIM Export Metadata tool to export the /db/oim-config.xml from the MDS repository. The OIM Export Metadata Tool, weblogicExportMetadata.sh is located under the *IAM_ORACLE_HOME/server/bin* directory.

2. Before you attempt to execute the tool, update the `weblogic.properties` file under the `IAM_ORACLE_HOME/server/bin` directory as follows:

```
# Weblogic Server Name on which OIM application is running

wls_servername=wls_oim1

# If you are importing or exporting any out of box event handlers, value is
oim.
# For rest of the out of box metadata, value is OIMMetadata.
# If you are importing or exporting any custom data, always use application
name as OIMMetadata.

application_name=oim

# Directory location from which XML file should be imported.
# Lets say I want to import User.xml and it is in the location
/scratch/asmaram/temp/oim/file/User.xml,
# I should give from location value as /scratch/asmaram/temp/oim. Make sure no
other files exist
# in this folder or in its sub folders. Import utility tries to recursively
import all the files under the
# from location folder. This property is only used by weblogicImportMetadata.sh

metadata_from_loc=@metadata_from_loc

# Directory location to which XML file should be exported to

metadata_to_loc=/home/oracle/oim_export

# For example /file/User.xml to export user entity definition. You can specify
multiple xml files as comma separated values.
# This property is only used by weblogicExportMetadata.sh and
weblogicDeleteMetadata.sh scripts
metadata_files=/db/oim-config.xml

# Application version
application_version=11.1.1.3.0
```

3. Set the `OIM_ORACLE_HOME` variable to the Identity Management Oracle Home.

```
prompt> export OIM_ORACLE_HOME=/u01/app/oracle/product/fmw/iam
```

4. Run the OIM Export Metadata Tool:

```
prompt> ./weblogicExportMetadata.sh
```

5. Provide the values for the username, password and the server URL when prompted.

```
Please enter your username [weblogic] :Enter the admin user name for the
Weblogic Domain, For Example: weblogic
Please enter your password [welcome1] : Enter the password for the Admin User
Please enter your server URL [t3://localhost:7001] Enter the URL to connect to
Admin Server. For Example:t3://oimhost1.mycompany.com:14000
```

6. The output from the tool will be similar to this:

```
Initializing WebLogic Scripting Tool (WLST) ...
```

```
Welcome to WebLogic Server Administration Scripting Shell
```

Type help() for help on available commands

```
Starting export metadata script ...
Please enter your username [weblogic] :weblogic
Please enter your password [welcome1] :
Please enter your server URL [t3://localhost:7001]
:t3://strasha14.us.oracle.com:14000
Connecting to t3://strasha14.us.oracle.com:14000 with userid weblogic ...
Successfully connected to managed Server 'wls_oim2' that belongs to domain
'IDMDomain'.
```

```
Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.
```

```
Location changed to custom tree. This is a writable tree with No root.
For more help, use help(custom)
```

```
Disconnected from weblogic server: wls_oim2
End of export metadata script ...
```

Exiting WebLogic Scripting Tool.

7. Edit the `oim-config.xml` file created under the `/home/oracle/oim_export/db` directory and update the value of `webgateType` to `ohsWebgate10g` as shown:

```
<webgateType>ohs10gwebgate</webgateType>
```

8. Update the `weblogic.properties` file under the `IAM_ORACLE_HOME/server/bin` directory as shown here:

```
# Weblogic Server Name on which OIM application is running

wls_servername=wls_oim1

# If you are importing or exporting any out of box event handlers, value is
oim.
# For rest of the out of box metadata, value is OIMMetadata.
# If you are importing or exporting any custom data, always use application
name as OIMMetadata.

application_name=oim

# Directory location from which XML file should be imported.
# Lets say I want to import User.xml and it is in the location
/sratc/asmaram/temp/oim/file/User.xml,
# I should give from location value as /sratc/asmaram/temp/oim. Make sure no
other files exist
# in this folder or in its sub folders. Import utility tries to recursively
import all the files under the
# from location folder. This property is only used by weblogicImportMetadata.sh

metadata_from_loc=/home/oracle/oim_export

# Directory location to which XML file should be exported to

metadata_to_loc=/home/oracle/oim_export
```

```
# For example /file/User.xml to export user entity definition. You can specify
multiple xml files as comma separated values.
# This property is only used by weblogicExportMetadata.sh and
weblogicDeleteMetadata.sh scripts
```

```
metadata_files=/db/oim-config.xml
```

```
# Application version
application_version=11.1.1.3.0
```

9. Run the OIM Import Metadata Tool:

```
prompt>./weblogicImportMetadata.sh
```

10. Provide the values for the username, password and the server URL when prompted.

```
Please enter your username [weblogic] :Enter the admin user name for the
Weblogic Domain, For Example: weblogic
Please enter your password [welcome1] : Enter the password for the Admin User
Please enter your server URL [t3://localhost:7001] Enter the URL to connect to
Admin Server. For Example:t3://ADMINVHN.mycompany.com:7001
```

11. The output from the tool will be similar to this:

```
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

Starting export metadata script ....
Please enter your username [weblogic] :weblogic
Please enter your password [welcome1] :
Please enter your server URL [t3://localhost:7001]
:t3://strasha14.us.oracle.com:14000
Connecting to t3://strasha14.us.oracle.com:14000 with userid weblogic ...
Successfully connected to managed Server 'wls_oim2' that belongs to domain
'IDMDomain'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or Admin port should be
used instead.

Location changed to custom tree. This is a writable tree with No root.
For more help, use help(custom)

Disconnected from weblogic server: wls_oim2
End of import metadata script ...
Exiting WebLogic Scripting Tool.
```

12. Stop and Start the Oracle Identity Management Managed Servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

17.6 Integrating Oracle Adaptive Access Manager with Oracle Access Manager

This section describes how to integrate OAAM with OAM and OIM. Once OAAM has been integrated with OAM, you can use OAAM instead of the standard OAM login to

validate access to resources. Even though OAAM is performing the authentication, it is authenticating against users in OAM.

When OAAM is integrated with OIM, OIM is used to help users who have forgotten their username or password.

17.6.1 Prerequisites

Before starting this association, ensure that the following tasks have been performed:

1. Install and configure Oracle Access Manager (OAM) as described in [Chapter 11](#).
2. Configure Oracle Access Manager to work with an LDAP store as described in [Section 11.7](#).
3. Install Oracle Adaptive Access Manager as described in [Chapter 12](#)

17.6.2 Configuring OAM Encryption Keys in CSF

1. Go to the Oracle Fusion Middleware Enterprise Manager console at `http://adminhost.us.oracle.com/em` using a web browser.
2. Log in using the WebLogic administrator account, for example `WebLogic`.
3. Expand the **WebLogic Domain** icon in the navigation tree in the left pane.
4. Select the `IDMDomain`, right click, and select the menu option **Security** and then the option "**Credentials** in the sub menu.
5. Click **oaam** to select the map, then click **Create Key**.
6. In the pop-up window make sure **Select Map** is **oaam**.
7. Enter:
 - **Key Name:** `oam.credentials`
 - **Type:** `Password`
 - **UserName:** `OAM`
 - **Password:** Password for OAM webgate
8. Click **OK** to save the secret key to the Credential Store Framework.

17.6.3 Configuring OAM Policy Authentication Scheme

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **Policy Configuration** tab.
3. Double click **OAAMAdvanced** under **Authentication Schemes**.
4. Enter the following information:
Challenge URL: `https://mysso.mycompany.com:443/oam_server/oamLoginPage.jsp`
5. Click **Apply**.

17.6.4 Setting OAAM properties for OAM

Oracle Adaptive Access Manager can use LDAP for user authentication. You enable this integration by using the OAAM administration console at `http://admin.mycompany.com/oaam_admin`.

Log in using the `oaamadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP"](#). Then proceed as follows:

1. In the Navigation Tree, click **Environment** and double click **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 **Value**.
Enter the new value and click **Save**.
4. Set the following properties to enable OAAM to integrate with OAM:
 - **bharosa.uio.default.password.auth.provider.classname:** `com.bharosa.vcrypt.services.OAMOAAAMAuthProvider`
 - **bharosa.uio.default.is_oam_integrated:** `true`
 - **oaam.uio.oam.host:** `idmhost1.mycompany.com`
 - **oaam.uio.oam.port:** OAM server proxy port, for example: `5574`
 - **oaam.uio.oam.obsso_cookie_domain:** `mycompany.com`
 - **oaam.uio.oam.webgate_id:** `Webgate_mysso`
 - **oaam.uio.oam.secondary.host:** `idmhost2.mycompany.com`
 - **oaam.uio.oam.secondary.host.port:** `3004`
 - **oaam.oam.csf.credentials.enabled:** `true`
 - **oaam.uio.login.page:** `/oamLoginPage.jsp`
5. Restart Managed Servers: Admin Server, `WLS_OAM1`, `WLS_OAM2`, `WLS_OAAM1`, and `WLS_OAAM2`, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

17.6.5 Validating Oracle Adaptive Access Manager/Oracle Identity Manager Integration

To perform this validation, first create a test resource

Create a test page called `oaam_sso.html` on `WEBHOST1` and `WEBHOST2`. The easiest way to do this is to create a file called `oaam_sso.html` in the directory `ORACLE_INSTANCE/config/OHS/component/htdocs` with the following:

```
<html>
<body>
<center>
<p>
<h2>
OAAM Protected Resource
</h2>
</p>
</center>
</body>
```

</html>

17.6.5.1 Creating a Resource

Now that you have something to protect, create a resource in OAM and assign it to the OAAM policy group you created in [Section 11.8.2, "Creating Oracle Adaptive Access ManagerPolicy Group"](#)

Log in to the OAM console at: `http://admin.mycompany.com`. Log in using the `oamadmin` account created previously.

1. From the Navigation window expand: **Application Domains > IDMDomainAgent**.
2. Click **Resources**.
3. Click **Create** on the tool bar below the **Browse** tab.
4. Enter the following information:
 - **Type:** `http`
 - **Host Identifier:** `IDMDomain`
 - **Resource URL:** `/oaam_sso.html`
5. Click **Apply**.

17.6.5.2 Assigning Resource to Policy Group

Now that the resource exists, assign it to one of the policy groups you created.

Log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account you previously created.

1. From the Navigation window, expand: **Application Domains > IDMDomainAgent > Authentication Policies**.
2. Click **OAAM Protected Resources**.
3. Click **Edit** on the tool bar below the **Browse** tab.
4. In the Resources box, click **+**.
5. From the list select, the resource you created.
6. Click **Apply**.

17.6.5.3 Adding Resource to Protected Resources

All that remains is to add the resource to the list of protected resources. To do this, log in to the OAM console at: `http://admin.mycompany.com` using the `oamadmin` account you created.

1. From the Navigation window expand: **Application Domains > IDMDomainAgent > Authorization Policies**.
2. Click **Protected Resource Policy**.
3. Click **Edit** on the tool bar below the **Browse** tab.
4. In the Resources box, click **+**.
5. From the list, select the resource you created.
6. Click **Apply**.

17.6.5.4 Validating Oracle Access Manager

Install Oracle WebGate as described in [Section 17.2, "Installing and Configuring WebGate"](#).

Access your protected resource using the URL:

`https://sso.mycompany.com:443/oaam_sso.html`. The OAAM Login page is displayed. Log in using an authorized OAM user such as `oamadmin`. Once you are logged in, the oaam protected resource is displayed.

17.7 Integrating Oracle Adaptive Access Manager with Oracle Identity Manager

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 allows 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 allows policies to be set based on the accounts owned, in addition to simple attributes.

In an Identity Management Suite 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 allows 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.

17.7.1 Prerequisites

Before starting this association, ensure that the following tasks have been performed:

1. Install and configure Oracle Identity Management.
2. Install Oracle Adaptive Access Manager.
3. Install and configure Oracle Access Manager.
4. Integrate Oracle Identity Manager with Oracle Access Manager, as described in [Section 17.4c](#)
5. Integrate Oracle Access Manager with Oracle Adaptive Access Manager as described in [Section 17.6](#).

17.7.2 Configuring OIM Encryption Keys in CSF

1. Go to Oracle Enterprise Manager Fusion Middleware Control at `http://adminhost.us.oracle.com/em` using a web browser.

2. Log in using the WebLogic administrator account, for example `WebLogic`.
3. Expand the `weblogic_domain` icon in the navigation tree in the left pane.
4. Select the IDM domain, right click, and select the menu option **Security** and then the option **Credentials** in the sub menu.
5. Click **Create Map**
6. Click `oaam` to select the map and then click **Create Key**.
7. In the pop-up window, make sure **Select Map** is `oaam`.
8. Enter:
 - **Key Name:** `oim.credentials`
 - **Type:** `Password`
 - **UserName:** `xelsysadm`
 - **Password:** Password for `xelsysadm` account,
9. Click **OK** to save the secret key to the Credential Store Framework

17.7.3 Setting OAAM properties for OIM

Go to the OAAM Administration Console at:

`http://OAAMHOST2.mycompany.com:14200/oaam_admin`.

Log in using the `oaamadmin` account you created in [Section 12.1.1, "Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP."](#) Then proceed as follows:

1. In the navigation tree, click **Environment** and double click **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 **Value**. Enter the new value and click **Save**.
4. Set the following properties to enable OAAM to integrate with OIM:
 - **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/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=SELF_REGISTRATION&backUrl=https://sso.us.oracle.com:443//oim/faces/pages/Self.jspx`
 - **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/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=UNAUTH_TRACK_REQUEST&backUrl=https://sso.us.oracle.com:443//oim/faces/pages/Self.jspx`
 - **oaam.oim.csf.credentials.enabled:** `true`

- **oaam.oim.auth.login.config:**
\${oracle.oaam.home}/../designconsole/config/authwl.conf
- **oaam.oim.url:** https://sso.mycompany.com:443
- **oaam.oim.xl.homedir:** \${oracle.oaam.home}/../designconsole

17.7.4 Setting OIM properties for OAAM

1. Log in to the OIM administrative console using the URL
`http://oimhost1.mycompany.com:14000/oim/self`.
2. Click the **Advanced** link on the self-service console
3. Click **System Properties** in the System Management Box.
4. Click **Advanced Search** below the System Configuration search box.
5. When the advanced search screen appears click **Search**. Do not provide a search string.
6. Click each the properties in the following list and set the value as shown. After setting each value, click **Save** to save the value:
 - `OIM.DisableChallengeQuestions:` TRUE
 - `OIM.ChangePasswordURL:`
`https://mysso.mycompany.com:443/oaam_server/oimChangePassword.jsp`
 - `OIM.ForgotPasswordURL:`
`https://mysso.mycompany.com:443/oaam_server/oimForgotPassword.jsp`
 - `OIM.ChallengeQuestionModificationURL:`
`https://mysso.mycompany.com:443/oaam_server/oimResetChallengeQuestions.jsp`

17.7.5 Restarting Oracle Adaptive Access Manager and Oracle Identity Manager

Restart the managed servers WLS_OAAM1, WLS_OAAM2, WLS_OIM1 and WLS_OIM2 as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

17.7.6 Restarting Managed Servers

Restart the following managed servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

- Admin Server
- WLS_OAM1 and WLS_OAM2
- WLS_OIM1 and WLS_OIM2
- WLS_OAAM1 and WLS_OAAM2

17.7.7 Validating OIM/OAAM Integration

Validate that OIM is integrated with OAAM as follows:

- Log in to OIM console at the URL:
`http://sso.mycompany.com:443/oim/self`.

The OAM login page is displayed.

- Log in to the OIM console as the `xelsysadm` user.

You are prompted to set up challenge questions and OAAM-specific security pictures.

17.8 Integrating Oracle Identity Federation with Oracle Access Manager

This section describes how to integrate Oracle Identity Federation with Oracle Access Manager.

17.8.1 Configure Oracle Identity Federation Server

You configure the Oracle Identity Federation server by using Oracle Enterprise Manager Fusion Middleware Control. Select the OIF target.

17.8.1.1 Generating and Configuring Identity Provider and Service Provider Modules

First, generate metadata.

1. From the OIF menu, select **Administration**, then **Security And Trust** and click the **Provider Metadata** tab.
2. In the Generate Metadata section of the page, select **Service Provider** and click **Generate** to generate metadata for the Service Provider.
3. Then select **Identity Provider** and click **Generate** to generate metadata for the Identity Provider.

Next, register the Service Provider and the Identity Provider by loading the metadata.

1. From the OIF menu, select **Administration**, then **Federations**.
2. Click **Add** to load the metadata you just generated.
3. Select **Enable Provider** and **Load Metadata**.

Both the Service Provider and the Identity Provider should now be listed on the Federations page.

17.8.1.2 Configuring the Data Stores

1. From the OIF menu, select **Administration**, then **Data Stores**.
2. Click **Edit**, select the **Repository Type**, and furnish the DataStore details in the **User Data Store** section of the page.

17.8.1.3 Configuring the Authentication Engines

1. From the OIF menu, select **Administration**, then **Authentication Engines**.
2. Furnish the Data Store settings configured in [Section 17.8.1.2, "Configuring the Data Stores"](#) here, so that the authentication engine has the details of the user data store to authenticate the user against.
3. Choose **LDAP Directory** in the Default Authentication Engine list. Click **Apply**.
4. From the OIF menu, select **Administration**, then **Service Provider**. On the **Common** tab, enable the Service Provider and choose the Service provider that was registered in [Section 17.8.1.1, "Generating and Configuring Identity Provider and Service Provider Modules"](#) as the Default Service Provider.

5. Similarly, from the OIF menu, select **Administration**, then **Identity Provider**.
6. On the **Common** tab, enable the Identity Provider and choose the Identity provider that was registered in [Section 17.8.1.1, "Generating and Configuring Identity Provider and Service Provider Modules"](#) as the Default Identity Provider.

17.8.1.4 Configuring the Oracle Identity Federation Server in Service Provider Mode

Now configure Oracle Identity Federation with the Oracle Access Manager Server details, so that it can send assertion tokens and leverage the session management to the Oracle Access Manager Server.

1. From the OIF menu, select **Administration**, then **Service Provider Integration Modules**.
2. Select **Oracle Single Sign-On** from the list.
3. On the **Oracle Single Sign-On** tab, select **Logout Enabled** and configure the following details:
 - Login URL: `http://oam_host:oam_port/ngam/server/dap/cred_submit`
 - Logout URL: `http://oam_host:oam_port/ngam/server/logout`
4. Next to **Oracle Single Sign-On Secret**, click **Regenerate**. This generates a file called `keystore` which contains the keys used to encrypt and decrypt tokens that pass between the Oracle Access Manager Server and the Oracle Identity Federation Server.
5. Generate the `keystore` file. Save the file when you get the Save As dialog box. Copy the `keystore` file into a location under the OAM Server Installation directory.

You will need to furnish the full path of the `keystore` file when you use the `wlst` command, as described in the next section.

17.8.2 Configuring Oracle Access Manager Server

In the previous section, you configured the OAM server to protect a resource. Now, whenever a user attempts to access the resource, the OAM Server challenges the user to furnish credentials. The next task is to configure OAM Server to leverage the authentication to the OIF Server.

Protect the resource with OIFScheme.

1. Copy the `keystore` file to a directory under the Middleware home in which the OAM Server is installed.
2. Invoke WLST and use the `registerOIFDAPPartner` command to update the `OIFDAPPartner` block in the `oamconfig.xml`, as follows:

```
registerOIFDAPPartner(keystoreLocation=location_of_keystore_file,
logoutURL=OIF_logout_URL)
```

where `OIF_logout_URL` is the URL to invoke when the Oracle Access Manager server logs out. For example:

```
registerOIFDAPPartner(keystoreLocation="/home/vaselvar/keystore",
logoutURL="http://oimhost1.us.oracle.com:7500/fed/user
/spsloosso?doneURL=http://sso.mycompany.com/oam/logout.jsp ")
```

3. To validate, open the `oam-config.xml` file, locate `OIFDAPPartner` and verify that the properties in that block are updated with those you supplied with the `wlst` command.
4. Next, edit the `oam-policy.xml` file in the `DOMAIN_HOME/config/fmwconfig` directory. Change the `OIFHost:OIFPort` to the relevant host port detail in the `OIFScheme`.

```
<authn-scheme version="1" type="allow" name="OIFScheme"
id="4bbbf36c-1781-49e0-bb42-7a5e8316450c" description="OIFScheme"
auth-level="2">
    <challenge-redirect-url>/ngam/server/</challenge-redirect-url>
    <challenge-mechanism>DAP</challenge-mechanism>
    <challenge-param>
        <param type="external" optional="false"
name="contextType"/>
        <param type="string" optional="false" name="daptoken"/>
        <param type="http://<OIFHost>:<OIF Port>/fed/user/sposso"
optional="false" name="challenge_url"/>
    </challenge-param>
    <authn-module name="DAP"/>
</authn-scheme>
```

5. Now add the federated user into the OAM Server's embedded LDAP.

Access the Administration Console at: `http://wls_host:wls_admin_port/console`.

Select **Security Realms > Users and Groups > New** then **Create a new user**.

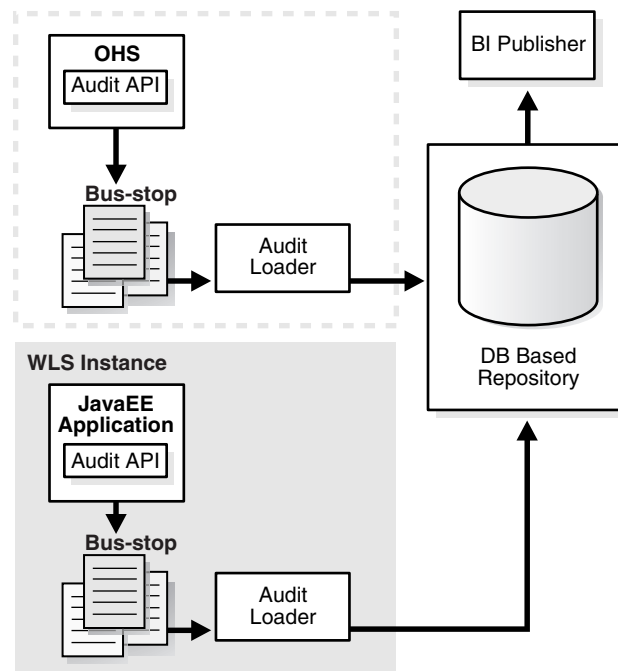
Note: The Data store you configured in [Section 17.8.1.2, "Configuring the Data Stores"](#) and the embedded LDAP must both contain this user.

6. Restart the Administration server and managed servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#)

17.9 Auditing Identity Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11g, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications will be able to create application-specific audit events. For non-JavaEE Oracle components in the middleware such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

[Figure 17-1](#) is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 17-1 Audit Event Flow

The Oracle Fusion Middleware Audit Framework consists of the following key components:

- **Audit APIs**

These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run-time, applications may call these APIs where appropriate to audit the necessary information about a particular event happening in the application code. The interface allows applications to specify event details such as username and other attributes needed to provide the context of the event being audited.

- **Audit Events and Configuration**

The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also allows applications to define application-specific events.

These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WLST (command-line tool).

- **The Audit Bus-stop**

Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are periodically uploaded to the audit repository based on a configurable time interval.

- **Audit Loader**

As the name implies, audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.

- Audit Repository

Audit Repository contains a pre-defined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and will grow overtime. Ideally, this should not be an operational database used by any other applications - rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (RAC) database as the audit data store.

- Oracle Business Intelligence Publisher

The data in the audit repository is exposed through pre-defined reports in Oracle Business Intelligence Publisher. The reports allow users to drill down the audit data based on various criteria. For example:

- Username
- Time Range
- Application Type
- Execution Context Identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware Application Security Guide*.

For information on how to configure the repository for Oracle Fusion Middleware Audit Framework, see the "Configuring and Managing Auditing" chapter in the *Oracle Fusion Middleware Application Security Guide*.

The EDG topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader will be available once the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

Managing Enterprise Deployments

This chapter provides information about managing the Identity Management enterprise deployment you have set up.

This chapter includes the following topics:

- [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#)
- [Section 18.2, "Monitoring Enterprise Deployments"](#)
- [Section 18.3, "Scaling Enterprise Deployments"](#)
- [Section 18.4, "Performing Backups and Recoveries"](#)
- [Section 18.5, "Patching Enterprise Deployments"](#)
- [Section 18.6, "Troubleshooting"](#)
- [Section 18.7, "Other Recommendations"](#)

18.1 Starting and Stopping Oracle Identity Management Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Identity Management.

18.1.1 Oracle Virtual Directory

Starting

Start system components such as Oracle Virtual Directory by typing:

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

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

Stopping

Stop system components such as Oracle Virtual Directory by executing the following command:

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

18.1.2 Oracle Internet Directory

Starting

Start system components such as Oracle Internet Directory by typing

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

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

Stopping

Stop system components such as Oracle Internet Directory by executing the following command:

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

18.1.3 Oracle HTTP Server

Prior to starting/stopping the Oracle HTTP server ensure that the environment variables `ORACLE_HOME` and `ORACLE_INSTANCE` are defined and that `ORACLE_HOME/opmn/bin` appears in the `PATH`. For example:

```
export ORACLE_HOME=/u01/app/oracle/product/fmw/web
export ORACLE_INSTANCE=/u01/app/oracle/admin/web[1-2]
export PATH=$ORACLE_HOME/opmn/bin:$PATH
```

Starting

Start the Oracle web tier by issuing the command:

```
opmnctl startall
```

Stop

Stop the web tier by issuing the command

```
opmnctl stopall
```

to stop the entire Web tier or

```
opmnctl stopproc process-type=OHS
```

to stop Oracle HTTP Server only.

Restarting

You can restart the web tier by issuing a `Stop` followed by a `Start` as described in the previous sections.

To restart the Oracle HTTP server only, use the following command.

```
opmnctl restartproc process-type=OHS
```

18.1.4 Node Manager

Start and stop the Node Manager as follows:

Starting

To start Node Manager, issue the commands:

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

Stopping

To stop node manager, kill the process started in the previous section

18.1.5 WebLogic Administration Server

Start and stop the WebLogic Administration Server as follows:

Starting

The recommended way to start the Administration server is to use WLST and connect to Node Manager:

```
IDMHOST1> cd ORACLE_BASE/product/fmw/oracle_common/common/bin
IDMHOST1> ./wlst.sh
```

Once in `wlst` shell, execute

```
wls:/offline>nmConnect(Admin_User,'Admin_Password',ADMINHOST1,'5556',
'IDMDomain','/u01/app/oracle/admin/domain_name/aserver/IDMDomain')
wls:/nm/domain_name> nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

Stopping

To stop the administration server, log in to the WebLogic console using the URL: `http://admin.mycompany.com:7001/console`.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click on the **Control** tab
3. Select **AdminServer(admin)**
4. Click **Shutdown** and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you wish to shutdown the administration server.

Restarting

Restart the server by following the Stop and Start procedures in the previous sections.

18.1.6 Oracle Identity Manager

Start and stop Oracle Identity Manager as follows:

Starting

To start the OIM managed server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com:7001/console`.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu

2. Click on the **Control** tab
3. Select **OIM Servers WLS_SOA1 and/or WLS_SOA2**

Note: Start the SOA managed servers (WLS_SOA1/WLS_SOA2) before starting the OIM managed servers (WLS_OIM1/WLS_OIM2).

4. Click on the **Start** button.
5. Click **Yes** when asked to confirm that you wish to start the server(s).
6. After WLS_SOA1 and/or WLS_SOA2 have started, select WLS_OIM1 and/or WLS_OIM2
7. Click **Start**.
8. Click **Yes** when asked to confirm that you wish to start the server(s).

Stopping

To stop the OIM managed server(s), log in to the WebLogic console using the URL: <http://admin.mycompany.com:7001/console>. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click the **Control** tab
3. Select **OIM Servers (WLS_OIM1 and/or WLS_OIM2) and WLS_SOA1 and/or WLS_SOA2**
4. Click the **Shutdown** button and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you wish to shutdown the server(s).

Restarting

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

18.1.7 Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as follows:

Starting

To start the OAM managed server(s), log in to the WebLogic console using the URL: <http://admin.mycompany.com:7001/console>.

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click on the **Control** tab
3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**
4. Click on the **Start** button.
5. Click **Yes** when asked to confirm that you wish to start the server(s).

Stopping

To stop the OAM managed server(s), log in to the WebLogic console using the URL: <http://admin.mycompany.com:7001/console>. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click the **Control** tab
3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**
4. Click the **Shutdown** button and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you wish to shutdown the server(s).

Restarting

Restart the server by following the `Stop` and `Start` procedures in the previous sections.

18.1.8 Oracle Adaptive Access Manager Managed Servers

Start and stop Oracle Adaptive Access Manager as follows:

Starting

To start the OAAM managed server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com:7001/console`. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click the **Control** tab
3. Select **OAAM Servers (WLS_OAAM1 and/or WLS_OAAM2)**
4. Click the **Start** button.
5. Click **Yes** when asked to confirm that you wish to start the server(s).

Stopping

To stop the OAM managed server(s), log in to the WebLogic console using the URL: `http://admin.mycompany.com:7001/console`. Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu
2. Click the **Control** tab
3. Select **OAAM Servers (WLS_OAAM1 and/or WLS_OAAM2)**
4. Click **Shutdown** and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you wish to shutdown the server(s).

Restarting

Restart the server by following the `Stop` and `Start` procedures above.

18.2 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity Management enterprise deployment described in this manual.

18.2.1 Monitoring Oracle Internet Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Internet Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware

components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.

2. The Identity and Access section below the chart includes the name of each individual Oracle Internet Directory instance (for example, oid1, oid2), its status, host name, and CPU usage percentage. A green arrow in the Status column indicates that the instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Internet Directory instance to view the home page for that instance.
3. The home page for an instance displays metrics for the instance such as performance, load, security, response, CPU utilization %, and memory utilization %.

18.2.1.1 Oracle Internet Directory Component Names Assigned by Oracle Identity Management Installer

When you perform an Oracle Internet Directory installation using Oracle Identity Management 11g Installer, the default component name that the installer assigns to the Oracle Internet Directory instance is oid1. You cannot change this component name.

The instance specific configuration entry for this Oracle Internet Directory instance is `cn=oid1, cn=osldapd, cn=subconfigsubentry`.

If you perform a second Oracle Internet Directory installation on another computer and that Oracle Internet Directory instance uses the same database as the first instance, the installer detects the previously installed Oracle Internet Directory instance on the other computer using the same Oracle database, so it gives the second Oracle Internet Directory instance a component name of oid2.

The instance specific configuration entry for the second Oracle Internet Directory instance is `cn=oid2, cn=osldapd, cn=subconfigsubentry`. Any change of properties in the entry `cn=oid2, cn=osldapd, cn=subconfigsubentry` will not affect the first instance (oid1).

If a third Oracle Internet Directory installation is performed on another computer and that instance uses the same database as the first two instances, the installer gives the third Oracle Internet Directory instance a component name of oid3, and so on for additional instances on different hosts that use the same database.

Note that the shared configuration for all Oracle Internet Directory instances is `cn=dsaconfig, cn=configsets, cn=oracle internet directory`. Any change in this entry will affect all the instances of Oracle Internet Directory.

This naming scheme helps alleviate confusion when you view your domain using Oracle Enterprise Manager by giving different component names to your Oracle Internet Directory instances.

18.2.2 Monitoring Oracle Virtual Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Virtual Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each instance of the Oracle Virtual Directory application (for example, ovd1, ovd2), its status, and host name. A green arrow in the Status column indicates that the Oracle

Virtual Directory instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Virtual Directory instance to view the home page for that instance.

3. The home page for an instance displays metrics and configurations for the instance such as:
 - Oracle Virtual Directory status - A green arrow next to the Oracle Virtual Directory instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.
 - Current Load - This indicates the current work load of this Oracle Virtual Directory instance. It includes three metrics: Open Connections, Distinct Connected Users, and Distinct Connected IP Addresses.
 - Average Response Time Metric - This displays the average time (in milliseconds) to complete an LDAP search request.
 - Operations Metric - This displays the average number of LDAP search requests finished per millisecond.
 - Listeners - This table lists the listeners configured for this Oracle Virtual Directory instance to provide services to clients.
 - Adapters - This table lists existing adapters configured with the Oracle Virtual Directory instance. Oracle Virtual Directory uses adapters to connect to different underlying data repositories.
 - Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the system resources consumed by the Oracle Virtual Directory instance.

18.2.3 Monitoring Oracle Directory Integration Platform

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Directory Integration Platform, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each instance of the Oracle Directory Integration Platform application (all have the name DIP (11.1.1.1.0)), its status, and host name. Each Oracle Directory Integration Platform instance is deployed in a different Managed Server). A green arrow in the Status column indicates that the Oracle Directory Integration Platform instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Directory Integration Platform instance to view the home page for that instance.
3. The home page for an instance displays metrics for the instance such as:
 - Oracle Directory Integration Platform status - A green arrow next to the Oracle Directory Integration Platform instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.
 - DIP Component Status - This table includes these metrics:

- Quartz Scheduler - This indicates whether tasks can be scheduled for synchronization or not. A green arrow indicates the scheduler is up and a red arrow indicates that the scheduler is down.
- Mbeans - This indicates whether profile management is available to the user or not. A green arrow indicates profile management is available and a red arrow indicates profile management is unavailable.
- Synchronization Profiles - This shows registered profiles and their execution status. In a high availability deployment, all the instances will show the same list of profiles.
- Provisioning Profiles- This shows registered provisioning profiles and their execution status. In a high availability deployment, all the instances will show the same list of profiles.
- Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the resource usage by the Oracle Directory Integration Platform instance.

18.2.4 Monitoring Oracle Access Manager

Oracle Enterprise Manager Grid Control can be used to perform monitoring of Oracle Access Manager. For details, see the "Identity Management" chapter of *Oracle Enterprise Manager Concepts*.

18.3 Scaling Enterprise Deployments

The reference enterprise topology discussed in this manual is highly scalable. It can be scaled up and or scaled out. When the topology is scaled up, a new server instance is added to a node already running one or more server instances. When the topology is scaled out, new servers are added to new nodes.

18.3.1 Scaling Up the Topology

The Oracle Identity Management topology described in the guide has three tiers: the directory tier, application tier and web tier. The components in all the three tiers can be scaled up by adding a new server instance to a node that already has one or more server instances running.

18.3.1.1 Scaling Up the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled up on one or both the nodes.

18.3.1.1.1 Scaling Up Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Internet Directory instance.

To add a new Oracle Internet Directory instance to either Oracle Internet Directory node, follow the steps in [Section 7.2.2, "Configuring an Additional Oracle Internet Directory Instance"](#) with the following variations:

1. In step 2 and step 4, choose ports other than 389 and 636 since these ports are being used by the existing Oracle Internet Directory instance on the node.
2. In step 5, instead of running the Oracle Identity Management 11g Installer, use the Oracle Fusion Middleware 11g Identity Management Configuration Wizard since the `ORACLE_HOME` already exists. Run the `config.sh` script under the `ORACLE_HOME/bin` directory to bring up the configuration wizard and follow the remaining steps to add a new Oracle Internet Directory instance to the node.
3. The screens in steps 6, 8, 9, 18, and 19 in [Section 7.2.2, "Configuring an Additional Oracle Internet Directory Instance"](#) are related to a new install and will not be shown since the `ORACLE_HOME` is being shared.
4. Follow the steps in [Section 7.3.1, "Registering Oracle Internet Directory with the Oracle WebLogic Server Domain"](#) to register the new Oracle Internet Directory instance with the WebLogic Domain. Use the location for the new Oracle Internet Directory instance as the value for `ORACLE_INSTANCE`.
5. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

18.3.1.1.2 Scaling Up Oracle Virtual Directory The directory tier has two nodes (`OVDHOST1` and `OVDHOST2`), each running an Oracle Virtual Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Virtual Directory instance.

To add a new Oracle Virtual Directory instance to either Oracle Virtual Directory node, follow the steps in [Section 7.3.1, "Registering Oracle Internet Directory with the Oracle WebLogic Server Domain"](#) with the following variations:

1. In step 2 and step 4, choose ports other than 6501 and 7501 since these ports are being used by the existing Oracle Virtual Directory instance on the node.
2. In step 6, instead of running the Oracle Identity Management 11g Installer, use the Oracle Fusion Middleware 11g Identity Management Configuration Wizard since the `ORACLE_HOME` already exists. Run the `config.sh` script under the `ORACLE_HOME/bin` directory to bring up the configuration wizard and follow the remaining steps to add a new Oracle Virtual Directory instance to the node.
3. The screens in steps 7, 9, 10, 16 and 17 in [Section 7.2.2, "Configuring an Additional Oracle Internet Directory Instance"](#) are related to a new install and will not be shown since the `ORACLE_HOME` is being shared.
4. Follow the steps in [Section 7.3.1, "Registering Oracle Internet Directory with the Oracle WebLogic Server Domain"](#) to register the new Oracle Virtual Directory instance with the WebLogic Domain. Use the location for the new Oracle Virtual Directory instance as the value for `ORACLE_INSTANCE`.
5. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

18.3.1.2 Scaling Up the Application Tier

The application tier has two nodes (`IDMHOST1` and `IDMHOST2`) running Managed Servers for Oracle Directory Integration Platform and Oracle Directory Services Manager, two nodes (`OAMHOST1` and `OAMHOST2`) running the Oracle Access Manager Identity Server and Access Server, and an Administration node (`OAMADMINHOST`) running an instance of the Oracle Access Manager WebPass, Policy Manager, WebGate and Oracle HTTP Server.

18.3.1.2.1 Scaling Up Oracle Directory Integration Platform and Oracle Directory Services Manager

The application tier already has a node (IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager components. The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management Home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for the Oracle Oracle Directory Integration Platform and Oracle Directory Services Manager components.

Follow the steps in [Section 9.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster,"](#) with the following variations to scale up the topology for Oracle Directory Integration Platform and Oracle Directory Services Manager:

1. Use the Oracle Identity Management Configuration Assistant to scale up the topology. Run the `config.sh` script under the `ORACLE_HOME/bin` directory to bring up the configuration assistant.
2. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in [Chapter 5, "Configuring the Web Tier"](#) to complete this task.

18.3.1.2.2 Scaling Up Oracle Access Manager 10g With Oracle Access Manager, the new server instances need to be installed under a separate `ORACLE_HOME` location. Sharing `ORACLE_HOME`s between instances of Oracle Access Manager components is not supported.

To scale up the Identity Server, follow the instructions in [Section 10.3.1.2, "Installing the Second Identity Server on OAMHOST2."](#)

To scale up the Access Server, follow the instructions in [Section 10.4.2.2, "Starting the Access Server Installation."](#)

To scale up the WebPass, follow the instructions in [Section 10.3.3, "Installing WebPass on OAMADMINHOST."](#)

To scale up the WebGate, follow the instructions in [Section 10.4.3, "Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2."](#)

18.3.1.2.3 Scaling Up Oracle Access Manager 11g Scale up OAM as follows:

Log in to the Oracle WebLogic Server Administration Console at `http://admin.mycompany.com/console`.

1. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
2. Click on **Lock & Edit** from the Change Center menu.
3. Select an existing server on the host you wish to extend, for example: `WLS_OAM1`.
4. Click **Clone**.
5. Enter the following information:
 - **Server Name:** A new name for the server, for example: `WLS_OAM3`.
 - **Server Listen Address:** The name of the host on which the managed server will run.
 - **Server Listen Port:** The port the new managed server will use, this port must be unique within the host.

6. Click **OK**.
7. Click on the newly created server **WLS_OAM3**
8. Set the SSL listen port. This should be unique on the host that the managed server will be running on.
9. Click **Save**.
10. Disable host name verification for the new managed server. Before starting and verifying the **WLS_OAM3** managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `OAMHOSTn`.

If the source server from which the new one was cloned had already disabled hostname verification, these steps are not required, as the hostname 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**.
11. Click **Activate configuration** from the Change Center menu.

Register the new managed server with OAM. You now need to configure the new managed server now as an OAM server. You do this from the Oracle OAM console. Proceed as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
 - **Server Name:** `WLS_OAM3`
 - **Host:** Host that the server will run on
 - **Port:** Listen port that was assigned when the managed server was created
 - **OAM Proxy Port:** Port you want the OAM proxy to run on. This is unique for the host
 - **Proxy Server ID:** `AccessServerConfigProxy`
 - **Mode:** `Open`
6. Click **Coherence** tab.

Set **Local Port** to a unique value on the host.

Click **Apply**.

7. Click **Apply**.

You can now start the new managed server.

18.3.1.2.4 Scaling Up Oracle Adaptive Access Manager To scale up OAAM, use the same procedure for both the OAAM server and the OAAM Administration Server.

Log in to the Oracle WebLogic Server console at:

`http://admin.mycompany.com/console`. Then proceed as follows:

1. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
2. Click **Lock & Edit** from the Change Center menu.
3. Select an existing server on the host that you want to extend, for example: `WLS_OAAM1` or `WLS_OAAM_ADMIN1`.
4. Click **Clone**.
5. Enter the following information:
 - **Server Name:** A new name for the server, for example: `WLS_OAAM3`.
 - **Server Listen Address:** The name of the host on which the managed server will run.
 - **Server Listen Port:** The port the new managed server will use. This port must be unique within the host.
6. Click **OK**.
7. Click the newly-created server `WLS_OAAM3`.
8. Set the SSL listen port. This should be unique on the host that the managed server will be running on.
9. Click **Save**.
10. Disable host name verification for the new managed server. Before starting and verifying the `WLS_OAAM3` 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 `OAAMHOSTn`.

If the source server from which the new one was cloned had already disabled hostname verification, these steps are not required, as the hostname verification settings were propagated to the cloned server. To disable host name verification:

- a. In the Oracle Fusion Middleware Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- b. Expand the **Environment** node in the Domain Structure pane.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select `WLS_OAAM3` 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**.
11. Click **Activate configuration** from the Change Center menu.

You must now configure the new managed server now as an OAM server. You do this from the Oracle OAM console. Proceed as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions Menu.
5. Enter the following information:
 - **Server Name:** `WLS_OAM3`
 - **Host:** Host that the server will be running on
 - **Port:** Listen port that was assigned when the managed server was created.
 - **OAM Proxy Port:** Port you want the OAM proxy to run on. This is unique for each host.
 - **Proxy Server ID:** `AccessServerConfigProxy`.
 - **Mode:** `Open`
6. Click **Apply**.
7. Click **Coherence** tab.

Set **Local Port** to a unique value on the host.

8. Click **Apply**.

You can now start the Access server. In order for the server to be used, however, you must inform any Webgates of its existence. You do this as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **System Configuration** tab
3. Expand **Agents** -> **OAM Agents** -> **10g Agents**.
4. Double click the Webgate you want to change.
5. Add the new server to either the Primary or Secondary server list by clicking the Add + symbol.
6. Select the server name from the list.
7. Click **Apply**.

18.3.1.3 Scaling Up Oracle Identity Manager (Adding Managed Servers to Existing Nodes)

In this case, you already have a node that runs a managed server configured with SOA components. The node contains a Middleware home, an Oracle home (SOA) and a domain directory for existing managed servers.

You can use the existing installations (the Middleware home, and domain directories) for creating new `WLS_OIM` and `WLS_SOA` servers. There is no need to install the Oracle

Identity Manager and Oracle SOA Suite binaries in a new location, or to run pack and unpack.

Follow these steps for scaling up the topology:

1. Using the Administration Console, clone either the WLS_OIM1 or the WLS_SOA1 into a new managed server. The source managed server to clone should be one that already exists on the node where you want to run the new managed server.

To clone a managed server:

- a. Select **Environment** -> **Servers** from the Administration Console.
- b. Select the managed server that you want to clone (for example, WLS_OIM1 or WLS_SOA1).
- c. Select **Clone**.

Name the new managed server WLS_OIM n or WLS_SOA n , where n is a number to identify the new managed server.

The rest of the steps assume that you are adding a new server to OIMHOST1, which is already running WLS_SOA1 and WLS_OIM1.

2. For the listen address, assign the host name or IP address to use for this new managed server. If you are planning to use server migration as recommended for this server, this should be the VIP (also called a floating IP) to enable it to move to another node. The VIP should be different from the one used by the managed server that is already running.
3. Create JMS Servers for SOA, OIM and UMS on the new managed server.
 - a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMServer and name it, for example, SOAJMSFileStore_ N . Specify the path for the store. This should be a directory on shared storage, as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

Note: This directory must exist before the managed server is started or the start operation fails.

`ORACLE_BASE/admin/DOMAIN_NAME/cluster_name/jms/SOAJMSFileStore_N`

- b. Create a new JMS server for SOA, for example, SOAJMServer_ N . Use the SOAJMSFileStore_ N for this JMSServer. Target the SOAJMServer_ N server to the recently created managed server (WLS_SOA n).
- c. Create a new persistence store for the new UMSJMSServer, for example, UMSJMSFileStore_ N Specify the path for the store. This should be a directory on shared storage as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

`ORACLE_BASE/admin/domain_name/cluster_name/jms/UMSJMSFileStore_N.`

Note: This directory must exist before the managed server is started or the start operation fails. You can also assign SOAJMSFileStore_ N as store for the new UMS JMS servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- d. Create a new JMS Server for UMS, for example, `UMSJMSserver_N`. Use the `UMSJMSfileStore_N` for this JMS Server. Target the `UMSJMSserver_N` server to the recently created Managed Server (`WLS_SOAn`).
- e. Create a new persistence store for the new `OIMJMSserver`, for example, `OIMJMSfileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

`ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSfileStore_N`

Note: This directory must exist before the managed server is started or the start operation fails. You can also assign `SOAJMSfileStore_N` as store for the new `OIM JMS Servers`. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- f. Create a new JMS Server for OIM, for example, `OIMJMSserver_N`. Use the `OIMJMSfileStore_N` for this JMS Server. Target the `OIMJMSserver_N` server to the recently created Managed Server (`WLS_OIMn`).
- g. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for `SOAJMSModule` appears. Click the **SubDeployments** tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of `SOAJMSserverXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `SOAJMSserverXXXXXX` subdeployment. Add the new JMS Server for SOA called `SOAJMSserver_N` to this subdeployment. Click **Save**.

- h. Update the SubDeployment targets for the `UMSJMSsystemResource` to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSsystemResource** (represented as a hyperlink in the **Names** column of the table). The Settings page for `UMSJMSsystemResource` appears. Click the **SubDeployments** tab. The subdeployment module for **UMSJMS** appears.

Note: This subdeployment module name is a random name in the form of `UCMJMSserverXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `UMSJMSserverXXXXXX` subdeployment. Add the new JMS Server for UMS called `UMSJMSserver_N` to this subdeployment. Click **Save**.

- i. Update the SubDeployment targets for OIMJMSModule to include the recently created OIM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for OIMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for OIMJMS appears.

Note: This subdeployment module name is a random name in the form of OIMJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_OIM1 and WLS_OIM2).

Click the OIMJMSServerXXXXXX subdeployment. Add the new JMS Server for OIM called OIMJMSServer_N to this subdeployment. Click **Save**.

4. Configure Oracle Coherence for deploying composites, as described in Section "Configuring Oracle Coherence for Deploying Composites."

Note: Only the localhost field needs to be changed for the server. Replace the localhost with the listen address of the new server added, for example: Dtangosol.coherence.localhost=SOAHOST1VHNn

5. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

From the Administration Console, select the **Server_name > Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

6. Disable host name verification for the new managed server. Before starting and verifying the WLS_SOAn managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in SOAHOSTn. If the source server from which the new one has been cloned had already disabled hostname verification, these steps are not required (the hostname verification settings is propagated to the cloned server).

To disable host name verification:

- a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- b. Expand the **Environment** node in the Domain Structure window.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select **WLS_SOAn** in the Names column of the table. The Settings page for the server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to None.
- h. Click **Save**.

7. 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_SOAn`, is up.
 - c. Access the application on the newly created managed server (`http://vip:port/soa-infra`). The application should be functional.
8. Test server migration for this new server. Follow these steps from the node where you added the new server:
 - a. Stop the `WLS_SOAn` 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_SOAn` has been disabled.
 - c. Wait for the Node Manager to try a second restart of `WLS_SOAn`. Node Manager waits for a fence period of 30 seconds before trying this restart.
 - 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.

18.3.1.4 Scaling Up the Web Tier

The web tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance. To scale up the Oracle HTTP Server, follow the steps in [Chapter 5, "Configuring the Web Tier."](#)

In addition copy any files created in `ORACLE_INSTANCE/config/OHS/component/moduleconf` from the existing web tier configuration to the new one.

1. Use the Oracle Fusion Middleware 11g Web Tier Utilities Configuration Wizard to scale up the topology. Run the `config.sh` script under the `ORACLE_HOME/bin` directory to bring up the configuration wizard and follow the remaining steps to create a new instance of the Oracle HTTP Server.
2. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

18.3.2 Scaling Out the Topology

In scaling out a topology, new servers are added to new nodes. The components in all three tiers of the Oracle Identity Management topology described in this manual can be scaled out by adding a new server instance to a new node.

18.3.2.1 Scaling Out the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (OVDHOST1 and OVDHOST2), each running an Oracle

Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled out by adding new nodes to the directory tier.

18.3.2.1.1 Scaling Out Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (OIDHOST1 and OIDHOST2), each running an Oracle Internet Directory instance. The OID instances can be scaled out by adding a new node to the existing Oracle Internet Directory cluster. To scale out Oracle Internet Directory instances, follow these steps:

1. Follow the steps in [Section 7.2.2, "Configuring an Additional Oracle Internet Directory Instance"](#) to add a new node running Oracle Internet Directory.
2. Follow the steps in [Section 7.3.1, "Registering Oracle Internet Directory with the Oracle WebLogic Server Domain"](#) to register the new Oracle Internet Directory instance with the WebLogic domain.
3. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

18.3.2.1.2 Scaling Out Oracle Virtual Directory The directory tier has two nodes (OVDHOST1 and OVDHOST2), each running an Oracle Virtual Directory instance. Oracle Virtual Directory can be scaled out by adding a new node configured to run Oracle Virtual Directory to the directory tier. To scale out Oracle Virtual Directory instances, follow these steps:

1. Follow the steps in [Section 8.2.2, "Configuring an Additional Oracle Virtual Directory"](#) to add a new node running Oracle Virtual Directory.
2. Follow the steps in [Section 8.3.1, "Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain"](#) to register the new Oracle Virtual Directory instance with the WebLogic domain.
3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

18.3.2.2 Scaling Out the Application Tier

The application tier has two nodes (IDMHOST1 and IDMHOST2) running Managed Servers for Oracle Directory Integration Platform and Oracle Directory Services Manager, two nodes (OAMHOST1 and OAMHOST2) running the Oracle Access Manager Identity Server and Access Server, and an Administration node (OAMADMINHOST) running an instance of the Oracle Access Manager WebPass, Policy Manager, WebGate and Oracle HTTP Server.

18.3.2.2.1 Scaling Out Oracle Directory Integration Platform and Oracle Directory Services Manager The application tier has two nodes (IDMHOST1 and IDMHOST2) running a Managed Server configured with Oracle Directory Integration Platform and Oracle Directory Services Manager. The Oracle Directory Integration Platform and Oracle Directory Services Manager instances can be scaled out by adding a new node with a Managed Server to the existing cluster. To scale out DIP and ODSM instances, follow the steps below:

1. Follow the steps in [Section 9.2, "Expanding the Oracle Directory Integration Platform and ODSM Cluster"](#) to scale out the Oracle Directory Integration Platform and Oracle Directory Services Manager instances in the topology.
2. Reconfigure the Oracle HTTP Server module with the new Managed Server. See [????](#) for the instructions to complete this task.

18.3.2.2.2 Scaling Out Oracle Access Manager 10g With Oracle Access Manager, the new server instances need to be installed under a separate ORACLE_HOME location. Sharing ORACLE_HOMEs between instances of Oracle Access Manager components is not supported.

To scale out the Access Server, follow the instructions in [Section 10.4.2.2, "Starting the Access Server Installation."](#)

To scale out the WebPass, follow the instructions in [Section 10.3.3, "Installing WebPass on OAMADMINHOST."](#)

To scale out the WebGate, follow the instructions in [Section 10.4.3, "Installing WebGate on OAMADMINHOST, WEBHOST1, and WEBHOST2."](#)

18.3.2.2.3 Scaling Out Oracle Access Manager 11g Scale out is very similar to scale up but first requires the software to be installed on the new node.

1. Install Oracle WebLogic Server on the new host as described in [Section 4.5.3, "Installing Oracle WebLogic Server."](#)
2. Install Oracle Fusion Middleware Identity Management components on the new host as described in [Section 4.5.4, "Installing the Oracle Identity Management Platform and Directory Services Suite."](#)
3. Log in to the Oracle WebLogic Server Administration Console at `http://admin.mycompany.com/console`.
4. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
5. Click **Lock & Edit** from the Change Center menu.
6. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.
7. Click **Clone**.
8. Enter the following information:
 - **Server Name:** A new name for the server, for example: `WLS_OAM3`.
 - **Server Listen Address:** The name of the host on which the managed server will run.
 - **Server Listen Port:** The port the new managed server will use. This port must be unique within the host.
9. Click **OK**.
10. Click the newly created server `WLS_OAM3`.
11. Set the SSL listen port. This should be unique on the host that the managed server will run on.
12. Click **Save**.
13. Disable host name verification for the new managed server. Before starting and verifying the `WLS_OAM3` managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `IDMHOSTn`.

If the source server from which the new one was cloned had already disabled hostname verification, these steps are not required, as the hostname verification

settings was propagated to the cloned server. To disable host name verification, proceed as follows:

- a. In Oracle Enterprise Manager Fusion Middleware Control, select Oracle WebLogic Server Administration Console.
 - b. Expand the **Environment** node in the Domain Structure pane.
 - c. Click **Servers**. The Summary of Servers page appears.
 - d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.
 - e. Click the **SSL** tab.
 - f. Click **Advanced**.
 - g. Set **Hostname Verification** to **None**.
 - h. Click **Save**.
14. Click **Activate Configuration** from the Change Center menu.
15. Pack the domain on IDMHOST1 using the command:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/tmp/IDMDomain.jar -template_name="OAM Domain" -managed=true
```

The `pack.sh` script is located in `MW_HOME/oracle_common/common/bin`.

16. Unpack the domain on the new host using the command:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain
-template=/tmp/IDMDomain.jar -template_name="OAM Domain" -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

The `unpack.sh` script is located in `MW_HOME/oracle_common/common/bin`.

17. Before you can start managed servers from the console, you must create a node manager properties file on IDMHOST3. You do this by running the script `setNMProps.sh`, which is located in `MW_HOME/oracle_common/common/bin`. Type:

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

Register the new managed server with OAM. The new managed server now needs to be configured as an OAM server. You do this from the Oracle OAM console, as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
 - **Server Name:** `WLS_OAM3`
 - **Host:** Host that the server will be running on, `IDMHOST3`.
 - **Port:** Listen port that was assigned when the managed server was created.
 - **OAM Proxy Port:** Port you want the OAM proxy to run on. This is unique for the host.

- **Proxy Server ID:** AccessServerConfigProxy
- **Mode:** Open

6. Click Apply.

You can now start the Access Server. In order for the server to be used, however, you must inform any Webgates of its existence. You do that as follows:

1. Log in to the OAM console at `http://admin.mycompany.com/oamconsole` as the `oamadmin` user.
2. Click the **System Configuration** tab.
3. Expand **Agents** -> **OAM Agents** -> **10g Agents**.
4. Double click the Webgate you want to change.
5. Add the new server to either the primary or secondary server list by clicking the Add [+] icon.
6. Select the server name from the list.
7. Click **Apply**.

Update the Web Tier. Now that the new managed server has been created and started, the web tier will start to direct requests to it. Best practice, however, is to inform the web server that the new managed server has been created.

You do this by updating the file `OAM.conf` on each of the web tiers. This file resides in the directory: `ORACLE_INSTANCE/config/OHS/component_name/moduleconf`.

Add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /OAM_admin>
  SetHandler weblogic-handler
  WebLogicCluster
OAMhost1.mycompany.com:14200,OAMhost2.mycompany.com:14200
</Location>
```

to:

```
<Location /OAM_admin>
  SetHandler weblogic-handler
  WebLogicCluster

OAMhost1.mycompany.com:14200,OAMhost2.mycompany.com:14200,OAMhsot3.mycompany.com:14300
</Location>
```

18.3.2.2.4 Scaling Out Oracle Adaptive Access Manager Scale out is very similar to scale up, but first requires the software to be installed on the new node. Proceed as follows:

1. Install Oracle WebLogic Server on the new host as described in [Section 4.5.3, "Installing Oracle WebLogic Server."](#)
2. Install Oracle Fusion Middleware Identity Management components on the new host as described in [Section 4.5.4, "Installing the Oracle Identity Management Platform and Directory Services Suite."](#)
3. Log in to the WebLogic console at `http://admin.mycompany.com/console`.

4. From the Domain Structure pane of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
5. Click **Lock & Edit** from the Change Center menu.
6. Select an existing server on the host you want to extend, for example: `WLS_OAAM1` or `WLS_OAAM_ADMIN1`.
7. Click **Clone**.
8. Enter the following information:
 - **Server Name:** A new name for the server, for example: `WLS_OAAM3`
 - **Server Listen Address:** The name of the host on which the managed server will run.
 - **Server Listen Port:** The port the new managed server will use. This port must be unique within the host.
9. Click **OK**.
10. Click the newly-created server `WLS_OAAM3`.
11. Set the SSL listen port. This should be unique on the host that the managed server will be running on.
12. Click **Save**.
13. Disable host name verification for the new managed server. Before starting and verifying the `WLS_OAAM3` 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 `OAAMHOSTn`.

If the source server from which the new one was cloned had already disabled hostname verification, these steps are not required, as the hostname verification settings were propagated to the cloned server. To disable host name verification:

- a. In the Oracle Fusion Middleware Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- b. Expand the **Environment** node in the Domain Structure pane.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select `WLS_OAAM3` in the Names column of the table. The Settings page for server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to `None`.
- h. Click **Save**.
14. Click **Activate configuration** from the Change Center menu.
15. Pack the domain on `IDMHOST1` using the command:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/tmp/IDMDomain.jar -template_name="OAAM Domain" -managed=true
```

The `pack.sh` script is located in `MW_HOME/oracle_common/common/bin`.
16. Unpack the domain on the new host using the command:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/mserver/IDMDomain
-template=/tmp/IDMDomain.jar -template_name="OAAM Domain" -app_dir=ORACLE_
BASE/admin/IDMDomain/mserver/applications
```

The `unpack.sh` script is located in `MW_HOME/oracle_common/common/bin`.

17. Before you can start managed servers from the console, you must create a node manager properties file on `OAAMHOST2` by running the script `setNMProps.sh`. The `setNMProps.sh` script is located in `MW_HOME/oracle_common/common/bin`. Type:

```
OAAMHOST2> $MW_HOME/oracle_common/common/bin/setNMProps.sh
```

18. Start Node Manager and the new managed server on the new host
19. Now that the new managed server has been created and started, the web tier will start to direct requests to it. Best practice, however, is to inform the web server that the new managed server has been created.

You do this by updating the file `oaam.conf` on each of the web tiers. This file resides in the directory: `ORACLE_INSTANCE/config/OHS/component_name/moduleconf`.

Add the new server to the `WebLogicCluster` directive in the file. For example, change:

```
<Location /oaam_admin>
  SetHandler weblogic-handler
  WebLogicCluster
oaamhost1.mycompany.com:14200,oaamhost2.mycompany.com:14200
</Location>
```

to:

```
<Location /oaam_admin>
  SetHandler weblogic-handler
  WebLogicCluster
oaamhost1.mycompany.com:14200,oaamhost2.mycompany.com:14200,oaamhsot3.mycompany
.com:14300
</Location>
```

18.3.2.3 Scaling Out Oracle Identity Manager (Adding Managed Servers to New Nodes)

When you scale out the topology, you add new managed servers configured with SOA to new nodes.

Before performing the steps in this section, check that you meet these requirements:

- There must be existing nodes running managed servers configured with SOA within the topology.
- The new node can access the existing home directories for WebLogic Server and SOA.

Use the existing installations in shared storage for creating a new `WLS_SOA` or `WLS_WSM` managed server. You do not need to install WebLogic Server or SOA binaries in a new location but you do need to run `pack` and `unpack` to bootstrap the domain configuration in the new node.

Notes:

- If there is no existing installation in shared storage, installing WebLogic Server and SOA in the new nodes is required as described in Section xxx, "Configuring High Availability for Oracle SOA Service Infrastructure and Component Service Engines.
- When an `ORACLE_HOME` or `WL_HOME` is shared by multiple servers in different nodes, Oracle recommends keeping the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the `oraInventory` in a node and "attach" an installation in a shared storage to it, use:

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

To update the Middleware home list to add or remove a `WL_HOME`, edit the `user_home/boa/beahomelist` file. See the following steps.

Follow these steps for scaling out the topology:

1. On the new node, mount the existing Middleware home, which should include the SOA installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.
2. To attach `ORACLE_HOME` in shared storage to the local Oracle Inventory, execute the following command:

```
SOAHOSTn> cd ORACLE_BASE/product/fmw/soa/  
SOAHOSTn> ./attachHome.sh -jreLoc ORACLE_BASE/fmw/jrockit_160_17_R28.0.0-655
```
3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME/boa/beahomelist` file and add `ORACLE_BASE/product/fmw` to it.
4. Log in to the Oracle WebLogic Administration Console.
5. Create a new machine for the new node that will be used, and add the machine to the domain.
6. Update the machine's Node Manager's address to map the IP address of the node that is being used for scale out.
7. Use the Oracle WebLogic Server Administration Console to clone `WLS_SOA1` into a new managed server. Name it `WLS_SOAn`, where `n` is a number.

Note: These steps assume that you are adding a new server to node `n`, where no managed server was running previously.

8. Assign the host name or IP address to use for the new managed server for the listen address of the managed server.
9. If you are planning to use server migration for this server (which Oracle recommends) this should be the VIP address (also called a floating IP address) for the server. This VIP address should be different from the one used for the existing managed server.

10. Create JMS servers for SOA, OIM (if applicable), and UMS on the new managed server.

- a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMS`Server` and name it, for example, `SOAJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#) For example:

```
ORACLE_BASE/admin/domain_name/cluster_
name/jms/SOAJMSFileStore_N
```

Note: This directory must exist before the managed server is started or the start operation fails.

- b. Create a new JMS Server for SOA, for example, `SOAJMSServer_N`. Use the `SOAJMSFileStore_N` for this JMS`Server`. Target the `SOAJMSServer_N` Server to the recently created managed server (`WLS_SOAN`).
- c. Create a new persistence store for the new UMSJMS`Server`, and name it, for example, `UMSJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

```
ORACLE_BASE/admin/domain_name/cluster_
name/jms/UMSJMSFileStore _N
```

Notes:

- This directory must exist before the managed server is started or the start operation fails.
 - It is also possible to assign `SOAJMSFileStore_N` as the store for the new UMS JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.
-

- d. Create a new JMS server for UMS: for example, `UMSJMSServer_N`. Use the `UMSJMSFileStore_N` for this JMS server. Target the `UMSJMSServer_N` server to the recently created managed server (`WLS_SOAN`).
- e. Create a new persistence store for the new OIMJMS`Server`, and name it, for example, `OIMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 2.4, "Shared Storage and Recommended Directory Structure."](#)

```
ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSFileStore_N
```

Notes:

- This directory must exist before the managed server is started or the start operation fails.
 - It is also possible to assign `SOAJMSFileStore_N` as the store for the new OIM JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.
-

- f. Create a new JMS Server for OIM: for example, `OIMJMSServer_N`. Use the `OIMJMSFileStore_N` for this JMS Server. Target the `OIMJMSServer_N` Server to the recently created managed server (`WLS_SOAn`).
- g. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for **SOAJMSModule** appears. Open the SubDeployments tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of `SOAJMSServer` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `SOAJMSServerXXXXXX` subdeployment. Add the new JMS Server for SOA called `SOAJMSServer_N` to this subdeployment. Click **Save**.

- h. Update the SubDeployment targets for `UMSJMSSystemResource` to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the **Names** column of the table). The Settings page for `UMSJMSSystemResource` appears. Open the **SubDeployments** tab. The subdeployment module for **UMSJMS** appears.

Note: This subdeployment module is a random name in the form of `UMSJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `UMSJMSServerXXXXXX` subdeployment. Add the new JMS Server for UMS called `UMSJMSServer_N` to this subdeployment. Click **Save**.

- i. Update the SubDeployment Targets for `OIMJMSModule` to include the recently created OIM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose JMS Modules from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for `OIMJMSSystemResource` appears. Click the **SubDeployments** tab. The subdeployment module for **OIMJMS** appears.

Note: This subdeployment module is a random name in the form of `OIMJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `OIMJMSXXXXXX` subdeployment. Add the new JMS Server for OIM called `OIMJMSServer_N` to this subdeployment. Click **Save**.

- 11. Run the `pack` command on `SOAHOST1` to create a template pack as follows:

```
SOAHOST1> cd ORACLE_COMMON_HOME/common/bin
SOAHOST1> ./pack.sh -managed=true -domain=MW_HOME/user_
projects/domains/soadomain/ -template=soadomaintemplateScale.jar -template_
name=soa_domain_templateScale
```

Run the following command on SOAHOST1 to copy the template file created to SOAHOSTN:

```
SOAHOST1> scp soadomaintemplateScale.jar oracle@SOAHOSTN:/ ORACLE_
BASE/product/fmw/soa/common/bin
```

Run the `unpack` command on SOAHOSTN to unpack the template in the managed server domain directory as follows:

```
SOAHOSTN> cd ORACLE_BASE/product/fmw/soa/common/bin

SOAHOSTN> ./unpack.sh -domain=ORACLE_BASE/product/fmw/user_
projects/domains/soadomain/ -template=soadomaintemplateScale.jar
```

12. Configure Oracle Coherence for deploying composites, as described in Section xxxx, "Configuring Oracle Coherence for Deploying Composites."

Note: Only the `localhost` field needs to be changed for the server. Replace the `localhost` with the listen address of the new server added, for example: `Dtangosol.coherence.localhost=SOAHOSTnVHN1`

13. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.
From the Administration Console, select **Server_name** > **Services** tab. Under **Default Store**, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.
14. Disable host name verification for the new managed server. Before starting and verifying the `WLS_SOAn` managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `SOAHOSTn`. If the source server from which the new one has been cloned had already disabled hostname verification, these steps are not required (the hostname verification setting is propagated to the cloned server).

To disable host name verification:

- a. Expand the **Environment** node in the **Domain Structure** window.
- b. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select `WLS_SOAn` in the **Names** column of the table.
The Settings page for server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to **None**.
- h. Click **Save**.

15. Start the Node Manager on the new node. To start the Node Manager, use the installation in shared storage from the existing nodes, and start Node Manager by passing the host name of the new node as a parameter as follows:

```
SOAHOSTN> WL_HOME/server/bin/startNodeManager new_node_ip
```

16. Start and test the new managed server from the Oracle WebLogic Server Administration Console:
 1. Shut down all the existing managed servers in the cluster.
 2. Ensure that the newly created managed server, `WLS_SOAn`, is running.
 3. Access the application on the newly created managed server (`http://vip:port/soa-infra`). The application should be functional.
17. Configure server migration for the new managed server.

Note: Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP address for the new SOA Managed Server is already present in the new node.

Configure server migration following these steps:

- a. Log into the Administration Console.
- b. In the left pane, expand **Environment** and select **Servers**.
- c. Select the server (represented as hyperlink) for which you want to configure migration from the **Names** column of the table. The Setting page for that server appears.
- d. Click the **Migration** tab.
- e. In the **Available** field, in the **Migration Configuration** section, select the machines to which to allow migration and click the right arrow.

Note: Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional managed server.

- f. Select the **Automatic Server Migration Enabled** option. This enables the Node Manager to start a failed server on the target node automatically.
- g. Click **Save**.
- h. Restart the Administration Server, managed servers, and Node Manager.
- i. Test server migration for this new server. Follow these steps from the node where you added the new server:

1. Abruptly stop the `WLS_SOAn` managed server.

2. To do this, run:

```
kill -9 pid
```

on the (PID) of the managed server. You can identify the PID of the node using:

```
ps -ef | grep WLS_SOAn
```

3. Watch the Node Manager Console. You should see a message indicating that floating IP address for `WLS_SOA1` has been disabled.
4. Wait for the Node Manager to try a second restart of `WLS_SOAn`. Node Manager waits for a fence period of 30 seconds before trying this restart.
5. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.

18.3.2.4 Scaling Out the Web Tier

The web tier has two nodes each running an instance of the Oracle HTTP Server. The Oracle HTTP Server components can be scaled out by adding a new node configured to run Oracle HTTP Server to the web tier. To scale out Oracle HTTP Server, follow the steps in these sections:

1. [Section 4.4, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2."](#)
2. [Chapter 5, "Configuring the Web Tier."](#)
3. Copy any files created in `ORACLE_INSTANCE/config/OHS/component/moduleconf` from the existing web tier configuration to the new one.

18.4 Performing Backups and Recoveries

[Table 18–1](#) shows the static artifacts to back up in the 11g Oracle Identity Management enterprise deployment.

Table 18–1 Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	RAC database hosts: INFRADBHOST1 INFRADBHOST2	User Defined	Directory Tier
MW_HOME (OID)	OIDHOST1 OIDHOST2	MW HOME: /u01/app/oracle/product/fmw ORACLE HOME: /u01/app/oracle/product/fmw/idm on both the OIDHOST1 and OIDHOST2	Directory Tier
MW_HOME (OVD)	OVDHOST1 OVDHOST2	MW HOME: /u01/app/oracle/product/fmw ORACLE HOME: /u01/app/oracle/product/fmw/idm on both the OVDHOST1 and OVDHOST2	Directory Tier

Table 18–1 (Cont.) Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier
MW_HOME (DIP, ODSM, Admin Server)	IDMHOST1	FMW HOME:	Application Tier
	IDMHOST2	/u01/app/oracle/product/fmw	
		DIP/ODSM ORACLE HOME: /u01/app/oracle/product/fmw/idm on both IDMHOST1 and IDMHOST2	
		ADMIN SERVER ORACLE HOME: /u01/app/oracle/product/fmw/idm on both IDMHOST1 and IDMHOST2	
MW_HOME (OHS)	WEBHOST1	MW HOME:	Web Tier
	WEBHOST2	/u01/app/oracle/product/fmw	
		ORACLE HOME: /u01/app/oracle/product/fmw/web on WEBHOST1	
		ORACLE HOME: /u01/app/oracle/product/fmw/web on WEBHOST2	
OAMADMINHOST (used for OAM administration)	OAMADMINHOST	MW HOME:	Application Tier
		/u01/app/oracle/product/fmw	
		OHS ORACLE HOME: /u01/app/oracle/product/fmw/web	
		WEBPASS HOME: /u01/app/oracle/product/fmw/oam/webcomponents/entity	
		POLICY MANAGER HOME: /u01/app/oracle/product/fmw/oam/webcomponents/access	
		WEBGATE HOME: /u01/app/oracle/product/fmw/oam/webgate	
OAM	OAMHOST1 OAMHOST2	ORACLE ACCESS MANAGER HOME:	Application Tier
		/u01/app/oracle/product/fmw/oam	
		IDENTITY SERVER HOME: /u01/app/oracle/product/fmw/oam/identity	
		ACCESS SERVER HOME: /u01/app/oracle/product/fmw/oam/access	
Install Related Files	Each host	OraInventory: ORACLE_BASE/orainventory /etc/oratab, /etc/orainst.loc user_home/bea/beahomelist (on hosts where WebLogic Server is installed) Windows registry: (HKEY_LOCAL/MACHINE/Oracle)	Not applicable.

Table 18–2 shows the runtime artifacts to back up in the 11g Oracle Identity Management enterprise deployment:

Table 18–2 Runtime Artifacts to Back Up in the Identity Management Enterprise Deployments

Type	Host	Location	Tier
DOMAIN HOME	IDMHOST1 IDMHOST2	ORACLE_BASE/admin/IDMDomain/aserver on both IDMHOST1 and IDMHOST2	Application Tier
Application Artifacts (ear and war files)	IDMHOST1 IDMHOST2	Look at all the deployments, including Oracle Directory Integration Platform and Oracle Directory Services Manager, through the WebLogic Server Administration Console to identify all the application artifacts.	Application Tier
INSTANCE HOME (OHS)	WEBHOST1 WEBHOST2	OHS INSTANCE HOME on WEBHOST1: /u01/app/oracle/admin/ohs_inst1 OHS INSTANCE HOME on WEBHOST2: /u01/app/oracle/admin/ohs_inst2	Web Tier
INSTANCE HOME (OHS)	OAMADMINHOST	OHS INSTANCE HOME on WEBHOST1: /u01/app/oracle/admin/ohs_inst/oamAdmin_ohs	Application Tier
OID INSTANCE HOME	OIDHOST1 OIDHOST2	OID INSTANCE HOME on OIDHOST1: /u01/app/oracle/admin/oid_inst1 OID INSTANCE HOME on OIDHOST2: /u01/app/oracle/admin/oid_inst2	Directory Tier
OVD INSTANCE HOME	OVDHOST1 OVDHOST2	OVD INSTANCE HOME on OVDHOST1: /u01/app/oracle/admin/ovd_inst1 OVD INSTANCE HOME on OVDHOST2: /u01/app/oracle/admin/ovd_inst2	Directory Tier
RAC Databases	INFRADBHOST1 INFRADBHOST2	User defined	Directory Tier
OAM	OAMHOST1 OAMHOST2 OAMADMINHOST	All the configurations are within the respective home directories described in this table. There are no instance homes.	Application Tier

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

18.5 Patching Enterprise Deployments

This section describes how to patch an Oracle Fusion Middleware patch file and how to patch Oracle Identity Management components with minimal down time.

18.5.1 Patching an Oracle Fusion Middleware Source File

For information on patching an Oracle Fusion Middleware source file, see the *Oracle Fusion Middleware Administrator's Guide*.

18.5.2 Patching Identity Management Components

To patch Oracle Identity Management components with minimal down time, it is recommended that you follow these guidelines:

1. Route the LDAP traffic from OIDHOST1 and OVDHOST1 to OIDHOST2 and OVDHOST2.
2. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST1 or OVDHOST1).

3. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
4. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
5. Test the patch.
6. Route the traffic to OIDHOST1 or OVDHOST1 again.
7. Verify the applications are working properly.
8. Route the LDAP traffic on OIDHOST2 and OVDHOST2 to OIDHOST1 and OVDHOST1.
9. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (OIDHOST2 or OVDHOST2).
10. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
11. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
12. Test the patch.
13. Route the traffic to both hosts on which the patch has been applied (OIDHOST1 and OIDHOST2, or OVDHOST1 and OVDHOST2).

18.6 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity Management enterprise deployment described in this manual.

18.6.1 Troubleshooting Oracle Internet Directory

This section describes some of the common problems that can arise with Oracle Internet Directory and the actions you can take to resolve the problem.

Problem

The Oracle Internet Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Internet Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to Oracle Internet Directory server

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

The LDAP application is receiving LDAP Error 53 (DSA Unwilling to Perform). When one of the database nodes goes down during the middle of the LDAP transaction, the Oracle Internet Directory server sends error 53 to the LDAP client

Solution

To see why the Oracle Internet Directory database node went down, see the Oracle Internet Directory logs in this location:

```
ORACLE_INSTANCE/diagnostics/logs/OID/oidldapd01s*.log
```

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

18.6.2 Troubleshooting Oracle Virtual Directory

This section describes some of the common problems that can arise with Oracle Virtual Directory and the actions you can take to resolve the problem:

Problem

The Oracle Virtual Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Virtual Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

Problem

The SSO/LDAP Application connection is lost to the Oracle Virtual Directory server.

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

18.6.3 Troubleshooting Oracle Directory Integration Platform

This section describes some of the common problems that can arise with Oracle Directory Integration Platform and the actions you can take to resolve the problem.

Problem

The instance is not working properly.

Solution

Check the respective log of the instance. For example, if the instance deployed in wls_ods1 is not running, then check the wls_ods1-diagnostic.log file.

Problem

Exceptions similar to the following are seen in Managed Server log files running the Oracle Directory Integration Platform application during a RAC failover:

```
RuntimeException:
[2008-11-21T00:11:10.915-08:00] [wls_ods] [ERROR] []
[org.quartz.impl.jdbcjobstore.JobStoreTX] [tid: 25] [userId: <anonymous>]
[ecid: 0000Hqy69UiFW7V6u3FCEH199aj0000009,0] [APP: DIP] ClusterManager: Error
managing cluster: Failed to obtain DB connection from data source
'schedulerDS': java.sql.SQLException: Could not retrieve datasource via JNDI
url 'jdbc/schedulerDS' java.sql.SQLException: Cannot obtain connection:
driverURL = jdbc:weblogic:pool:schedulerDS, props =
{EmulateTwoPhaseCommit=false, connectionPoolID=schedulerDS,
jdbcTxDataSource=true, LoggingLastResource=false,
dataSourceName=schedulerDS}.[]
Nested Exception: java.lang.RuntimeException: Failed to setAutoCommit to true
for pool connection
```

```
AuthenticationException while connecting to OID:
[2008-11-21T00:12:08.812-08:00] [wls_ods] [ERROR] [DIP-10581] [oracle.dip]
[tid: 11] [userId: <anonymous>] [ecid: 0000Hqy6m54FW7V6u3FCEH199ap0000000,0]
[APP: DIP] DIP was not able to get the context with the given details {}[[
javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid
Credentials]
```

Most of the exceptions will be related to the scheduler or LDAP, for example:

1. Could not retrieve datasource via JNDI url 'jdbc/schedulerDS'
java.sql.SQLException.
2. javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]

Solution

During a RAC failover, exceptions are seen in the Managed Server log files running the Oracle Directory Integration Platform application. These errors are thrown when the multi data sources configured on the WebLogic Server platform try to verify the health of the RAC database instances during failover. These are innocuous errors and can be ignored. The Oracle Directory Integration Platform application will recover and begin to operate normally after a lag of one or two minutes. For a RAC failover, there will be no Oracle Directory Integration Platform down time if one instance is running at all times.

18.6.4 Troubleshooting Oracle Directory Services Manager

This section describes some of the common problems that can arise with Oracle Directory Services Manager and the actions you can take to resolve the problem.

After you have logged into Oracle Directory Services Manager, you can connect to multiple directory instances from the same browser window.

Avoid using multiple windows of the same browser program to connect to different directories at the same time. Doing so can cause a Target unreachable error.

You can log into the same Oracle Directory Services Manager instance from different browser programs, such as Internet Explorer and Firefox, and connect each to a different directory instance.

If you change the browser language setting, you must update the session in order to use the new setting. To update the session, either disconnect the current server connection, refresh the browser page (either reenter the Oracle Directory Services Manager URL in the URL field and press enter or press F5) and reconnect to the same server, or quit and restart the browser.

Problem

You attempt to invoke Oracle Directory Services Manager from Oracle Enterprise Manager Fusion Middleware Control by selecting Directory Services Manager from the Oracle Internet Directory menu in the Oracle Internet Directory target, then Data Browser, Schema, Security, or Advanced.

Oracle Directory Services Manager does not open. You might see an error message.

Solution

This is probably an installation problem. See Oracle Fusion Middleware Installation Guide for Oracle Identity Management.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You will see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.
2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.
3. Make a connection to an Oracle Internet Directory server.
4. Work with the Oracle Internet Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.
5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.
6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Internet Directory.
7. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.
2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.
3. Re-establish a new connection to the Oracle Internet Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to Oracle Internet Directory and displays the message LDAP Server is down.

Solution

In a High Availability configuration where Oracle Directory Services Manager is connected to Oracle Internet Directory through a load balancer, Oracle Directory Services Manager reports that the server is down during failover from one instance of Oracle Internet Directory to another. In other configurations, this message might indicate that Oracle Internet Directory has been shut down and restarted. In either case, the connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Internet Directory instance that is using a RAC database. Oracle Directory Services Manager might display the message

LDAP error code 53 - Function not implemented.

Solution

This error can occur during failover of the Oracle Database that the Oracle Internet Directory instance is using. The connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

Problem

You must perform the steps below to configure Oracle HTTP Server to route Oracle Directory Services Manager requests to multiple Oracle WebLogic Servers in a clustered Oracle WebLogic Server environment.

Solution

Perform these steps:

1. Create a backup copy of the Oracle HTTP Server's httpd.conf file. The backup copy will provide a source to revert back to if you encounter problems after performing this procedure.
2. Add the following text to the end of the Oracle HTTP Server's httpd.conf file and replace the variable placeholder values with the host names and Managed Server port numbers specific to your environment. Be sure to use the `<Location /odsm/ >` as the first line in the entry. Using `<Location /odsm/faces >` or `<Location /odsm/faces/odsm.jspx >` can distort the appearance of the Oracle Directory Services Manager interface.

```
<Location /odsm/ >
SetHandler weblogic-handler
WebLogicCluster host-name-1:managed-server-port,host-name_2:managed_server_port
</Location>
```

3. Stop, then start the Oracle HTTP Server as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components"](#) to activate the configuration change.

Note: Oracle Directory Services Manager loses its connection and displays a session time-out message if the Oracle WebLogic Server in the cluster that it is connected to fails. Oracle Directory Services Manager requests will be routed to the secondary Oracle WebLogic Server in the cluster that you identified in the `httpd.conf` file after you log back in to Oracle Directory Services Manager.

Problem

Attempting to access Oracle Directory Services Manager using a web browser fails.

Solution

- Verify the Oracle Virtual Directory server is running. The Oracle Virtual Directory server must be running to connect to it from Oracle Directory Services Manager.
- Verify you entered the correct credentials in the Server, Port, User Name and Password fields. You can execute an `ldapbind` command against the target Oracle Virtual Directory server to verify the server, user name, and password credentials.
- Verify you are using a supported browser. Oracle Directory Services Manager supports the following browsers:
 - Internet Explorer 7
 - Firefox 2.0.0.2 and 3.0
 - Safari 3.1.2 (desktop)
 - Google Chrome 0.2.149.30

Note: While Oracle Directory Services Manager supports all of the preceding browsers, only Internet Explorer 7 and Firefox 2.0.0.2 are certified.

Problem

Oracle Directory Services Manager does not open after you attempt to invoke it from Oracle Enterprise Manager Fusion Middleware Control by selecting one of the options from the **Directory Services Manager** entry in the **Oracle Virtual Directory** menu in the Oracle Virtual Directory target.

Solution

This is probably an installation problem. See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You will see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.
2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.
3. Make a connection to an Oracle Virtual Directory server.

4. Work with the Oracle Virtual Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.
5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.
6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Virtual Directory. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.
2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.
3. Re-establish a new connection to the Oracle Virtual Directory server you were working with earlier.

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Virtual Directory instance that is using an Oracle RAC Database. Oracle Directory Services Manager might display the message `LDAP error code 53 - Function not implemented`.

Solution

This error can occur during failover of the Oracle Database that the Oracle Virtual Directory instance is using. The connection will be reestablished in less than a minute, and you will be able to continue without logging in again.

18.6.5 Troubleshooting Oracle Access Manager

Most of the manuals in the Oracle Access Manager 10.1.4.3 documentation set include a Troubleshooting appendix.

For troubleshooting information about a particular Oracle Access Manager component or feature, refer to the appropriate manual in the Oracle Access Manager 10.1.4.3 documentation set. See the "Road Map to Manuals" section in the *Oracle Access Manager Introduction* manual for a description of each manual in the Oracle Access Manager documentation set.

18.6.5.1 User is Redirected to the Login Screen After Activating Some Administration Console Changes

Problem

After configuring Oracle HTTP Server and the load balancing router to access the Oracle WebLogic Administration console, some activation changes cause redirection to the login screen for the WebLogic Server Administration Console.

Solution

This is the result of the Administration Console tracking changes made to ports, channels, and security settings made using the Administration Console. For certain changes the Console may redirect the user's browser to the Administration Server's

listen address. Activation is completed regardless of the redirection. It is not required to log in again; users can simply update the URL to the following and then access the Home page for the Administration Console directly:

```
admin.mycompany.com/console/console.portal
```

18.6.5.2 User is Redirected to the Administration Console's Home Page After Activating Some Changes

Problem

After configuring Oracle Access Manager, some activation changes cause redirection to the Administration Console Home page (instead of the context menu where the activation was performed).

Solution

This is expected when Oracle Access Manager single sign-on is configured and is a result of the redirections performed by the Administration Server. Activation is completed regardless of the redirection. If required, user should manually navigate again to the desired context menu.

18.6.5.3 Oracle Access Manager Configuration Tool Does Not Remove Invalid URLs

Problem

If the policy domain has an invalid or incorrect URL, running the OAM Configuration Tool with the correct URLs will not update the Policy Manager, even though the tool completes successfully.

Solution

The OAM Configuration Tool adds new URLs to an existing policy domain when run using an existing `app_domain` name. It does not remove any of the existing URLs. The Policy Manager Console must be used to remove any invalid URLs. Follow these steps to update the URLs in an existing policy domain:

1. Access the Policy Manager Console using the following URL:

```
http://hostname:port/access/oblix
```

For example, enter the following URL in your web browser:

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

2. When prompted, log in using the `administrator` user credentials.
3. On the landing page, click the **Policy Manager** link.
4. On the Policy Manager Console, click the **My Policy Domains** link.
5. On the My Policy Domains page, click the link for the appropriate policy domain.
6. On the Policy Domain page, select the **Resources** tab.
7. On the Resources page, select the valid or incorrect URLs and delete them.

18.7 Other Recommendations

This section describes some other recommendations for the Oracle Identity Management enterprise deployment.

18.7.1 Preventing Timeouts for SQL*Net Connections

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall so it does not time out these connections. If such a configuration is not possible, set the `SQLNET.EXPIRE_TIME=n` parameter in the `ORACLE_HOME/network/admin/sqlnet.ora` file on the database server, where `n` is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For RAC, set this parameter in all of the Oracle home directories.

Configuring Single Sign-on for Administration Consoles

This chapter describes how to configure single sign-on for administration consoles. The administration consoles referred to in the chapter title are:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console
- Oracle Access Manager Console
- Oracle Identity Manager Console
- Oracle APM Console
- Oracle Adaptive Access Manager Admin Console

This chapter includes the following topics:

- [Section 19.1, "Prerequisites"](#)
- [Section 19.2, "Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 10g"](#)
- [Section 19.3, "Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 11g"](#)

19.1 Prerequisites

Before configuring single sign-on, ensure that the following tasks have been performed.

1. Create a WebLogic administrative user in an LDAP directory, as described in [Section 19.1.1](#)

19.1.1 Creating WebLogic Administrative Users in an LDAP Directory

In an enterprise, it is typical to have a centralized Identity Management domain where all users, groups and roles are provisioned and multiple application domains (such as a SOA domain and WebCenter domain). The application domains are configured to authenticate using the central Identity Management domain.

By default, when the Oracle WebLogic Server is installed and configured, the WebLogic admin user is created in its local LDAP store with the username `weblogic`. For an enterprise deployment, it is required to have all users, groups provisioned in an LDAP user directory such as Oracle Internet Directory that is a part of the centralized Identity Management Domain. This section provides details for provisioning a new

administrator user and group for managing the Identity Management WebLogic Domain. This section describes the following:

- [Section 19.1.1.1, "Provisioning Admin Users and Groups in an LDAP Directory"](#)
- [Section 19.1.1.2, "Assigning the Admin Role to the Admin Group"](#)
- [Section 19.1.1.3, "Updating the boot.properties File on IDMHOST1 and IDMHOST2"](#)

19.1.1.1 Provisioning Admin Users and Groups in an LDAP Directory

As mentioned in the introduction to this section, users and groups from multiple WebLogic domains may be provisioned in a central LDAP user store. In such a case, there is a possibility that one WebLogic admin user may have access to all the domains within an enterprise. This is not a desirable situation. To avoid this, the users and groups provisioned must have a unique distinguished name within the directory tree. In this guide, the admin user and group for the IDM WebLogic Domain will be provisioned with the DNs below:

- Admin User DN:

```
cn=weblogic_idm,cn=Users,dc=mycompany,dc=com
```

- Admin Group DN:

```
cn=IDM Administrators, cn=Groups,dc=mycompany,dc=com
```

Follow the steps below to provision the admin user and admin group in Oracle Internet Directory:

1. Create an ldif file named `admin_user.ldif` with the contents shown below and then save the file:

```
dn: cn=weblogic_idm, cn=Users, dc=us, dc=mycompany, dc=com
orclsamaccountname: weblogic_idm
givenname: weblogic_idm
sn: weblogic_idm
userpassword: Welcome1
obver: 10.1.4.0
mail: weblogic_idm
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
uid: weblogic_idm
cn: weblogic_idm
description: Admin User for the IDM Domain
```

2. Run the `ldapadd` command located under the `ORACLE_HOME/bin/` directory to provision the user in Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f admin_user.ldif
```

3. Create an ldif file named `admin_group.ldif` with the contents shown below and then save the file:

```
dn: cn=IDM Administrators, cn=Groups, dc=us, dc=mycompany, dc=com
displayname: IDM Administrators
objectclass: top
```

```

objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_idm,cn=users,dc=mycompany,dc=com
cn: IDM Administrators
description: Administrators Group for the IDM Domain in OID

```

4. Run the `ldapadd` command located under the `ORACLE_HOME/bin/` directory to provision the group in Oracle Internet Directory. For example:

```

ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f admin_group.ldif

```

19.1.1.2 Assigning the Admin Role to the Admin Group

After adding the users and groups to Oracle Internet Directory, the group must be assigned the Admin role within the WebLogic domain security realm. This enables all users that belong to the group to be administrators for that domain. Follow the steps below to assign the Admin role to the Admin group:

1. Log into the WebLogic Administration Server Console.
2. In the left pane of the console, click **Security Realms**.
3. On the Summary of Security Realms page, click **myrealm** under the **Realms** table.
4. On the Settings page for **myrealm**, click the **Roles & Policies** tab.
5. On the Realm Roles page, expand the **Global Roles** entry under the **Roles** table. This brings up the entry for Roles. Click on the **Roles** link to bring up the Global Roles page.
6. On the Global Roles page, click the **Admin Role** to bring up the Edit Global Role page:
 - a. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.
 - b. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.
 - c. On the Edit Arguments Page, Specify **IDM Administrators** in the **Group Argument** field and click **Add**.
7. Click **Finish** to return to the Edit Global Rule page.
8. The **Role Conditions** table now shows the `IDM Administrators Group` as an entry.
9. Click **Save** to finish adding the Admin Role to the `IDM Administrators Group`.
10. Validate that the changes were successful by bringing up the WebLogic Administration Server Console using a web browser. Log in using the credentials for the `weblogic_idm` user.

19.1.1.3 Updating the `boot.properties` File on `IDMHOST1` and `IDMHOST2`

The `boot.properties` file for the Administration Server and the Managed Servers should be updated with the WebLogic admin user created in Oracle Internet Directory. Follow the steps below to update the `boot.properties` file.

For the Administration Server on `IDMHOST1`

1. On `IDMHOST1`, go the following directory:

```
ORACLE_BASE/admin/domainName/aserver/domainName/servers/serverName/security
```

For example:

```
cd ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/servers/AdminServer/security
```

2. Rename the existing `boot.properties` file.
3. Use a text editor to create a file called `boot.properties` under the security directory. Enter the following lines in the file:

```
username=adminUser  
password=adminUserPassword
```

For example:

```
username=weblogic_idm  
password=Password for weblogic_idm user
```

Note: When you start the Administration Server, the username and password entries in the file get encrypted.

For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

Stopping and Starting the Servers

1. Stop the Administration Server and the `wls_ods1` and `wls_ods2` managed Servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Verify that the server processes have been successfully stopped.
3. On `IDMHOST1`, start the WebLogic Administration Server using the `startWebLogic.sh` script located under the `ORACLE_BASE/admin/domainName/aserver/domainName/servers/serverName/security/bin` directory using the syntax below. This enables the standard output log messages shown on the screen to be written to the file specified in the `logfile` parameter:

```
./startWebLogic.sh >logfile 2>&1 &
```

For example:

```
./startWebLogic.sh > \  
ORACLE_  
BASE/admin/IDMDomain/aserver/IDMDomain/servers/AdminServer/logs/aserver.out\  
2>&1 &
```

4. Verify that the Administration Server has started up and then bring up the Administration Console using a web browser.
5. Log in using the credentials of the `weblogic_idm` user.
6. Start the `wls_ods1` and `wls_ods2` Managed Servers using the WebLogic Administration Console.

19.2 Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 10g

This section explains how to configure single sign-on for administration consoles using Oracle Access Manager 10g.

19.2.1 Prerequisites for Configuring Single Sign-On

Make sure that the following tasks have been performed before moving on to the next section:

1. Install and configure Oracle Access Manager as described in [Chapter 10](#).
2. Ensure that the policy protecting the Policy Manager ("/access") has been created and enabled. If this is not enabled, use the Policy Manager console to enable it, as described in [Section 19.2.1.1](#).
3. Determine the host identifier value. It is required for enabling single sign-on.

19.2.1.1 Enable the Policy Protecting the Policy Manager

Follow these steps to enable policy protecting the Policy Manager:

1. Open a web browser and bring up the Policy Manager Console using the following URL:

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

2. Click the **Policy Manager** link.
3. On the Policy Manager landing page, click the **My Policy Domains** link.
4. On the My Policy Domains page, click the **Policy Manager** link.
5. On the **General** tab on the Policy Manager page, click **Modify**.
6. Click **Yes** to enable the "/"access" policy.
7. Click the **Save** button to save the changes.

19.2.2 Updating the Form Authentication for Delegated Administration

The WebGates in the IDM Domain also need to act as delegated authentication WebGates, that is, they receive authentication requests from external applications or domains in the enterprise. To enable delegated authentication, the form authentication scheme created by the OAM Configuration Tool must be modified to add the Challenge Redirect parameter.

Follow the steps below to add the challenge redirect parameter to the Form authentication scheme:

1. Use a web browser to display the Access Console using the URL below:

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

2. Click the Access System Console link and log in using the credentials for the orcladmin user.
3. On the main page, click the Access System Configuration tab.
4. On the Access System Configuration page, click the **Authentication Management** link on the left hand side.

5. On the Authentication Management page, under the **List all Authentication Schemes** table, click the link for form authentication scheme created by the tool. The form authentication scheme created by the tool is called `OraDefaultFormAuthNScheme`.
6. On the Details for Authentication Scheme page, click **Modify** to modify the configuration of the authentication scheme.
7. On the Modifying Authentication Scheme page, update the Challenge Redirect parameter with the Single Sign-On virtual host configured in the load balancer. Use `https://sso.mycompany.com` to update the Challenge Redirect parameter.
8. Click **Save** to save the updated configuration.
9. To validate that the configuration was successful, follow the steps below:
 - a. Using a web browser, bring up either the Oracle WebLogic Administration Console or Oracle Enterprise Manager Fusion Middleware Control:
URL for the WebLogic Administration Server Console:
`http://admin.mycompany.com:7777/console`

URL for the Enterprise Manager Oracle Fusion Middleware Control:
`http://admin.mycompany.com:7777/em`
 - b. This will redirect your web browser to `https://sso.mycompany.com` for authentication.

Log into the console using the administrator user's credentials. For example: `orcladmin, password`.
 - c. Then you will be redirected back to the WebLogic Administration Console login page. Log in using `weblogic, password`.

19.2.3 Validating the Policy Domain and AccessGate Configurations

The next part of the process is to validate the policy domain configuration and the AccessGate configuration.

19.2.3.1 Validating the Policy Domain Configuration

Follow these steps to verify that the policy domain was created properly:

1. In a web browser, enter this URL to access the Oracle Access Manager console:
`http://oamadminhost.mycompany.com:port/access/oblix`
2. Click **Policy Manager**.
3. Click the **My Policy Domains** link on the left panel. You will see a list of all the policy domains, which includes the domain you just created. For example: `IDMEDG`. In the third column, **URL prefixes**, you will see the URIs you specified when creating the policy domain).
4. Click the link to the policy domain you just created. This displays the General area of this domain.
5. Click the Resources tab. On this tab you can see the URIs you specified. Click other tabs to view other settings.

19.2.3.2 Validating the AccessGate Configuration

Follow these steps to verify that the AccessGate was configured properly:

1. In the Oracle Access Manager console, click the **Access System Console** link. This link is a toggle. When it is the **Access System Console** link and you click it, it becomes the **Policy Manager** link. When it is the **Policy Manager** link and you click it, it becomes the **Access System Console** link.
2. Click the **Access System Configuration** tab.
3. Click the **AccessGate Configuration** link on the left panel.
4. Enter some search criteria and click **Go**.
5. When the name of the AccessGate for the domain you created appears (it may have the suffix `_AG` when created by the OAM Configuration Tool, for example, `IDMEDG_AG`), click it to view the details of the AccessGate you created.

19.2.4 Setting Up the WebLogic Authenticators

This section describes the steps for setting up Oracle WebLogic Server authenticators.

19.2.4.1 Setting Up the Oracle Internet Directory Authenticator

Follow these steps to set up the Oracle Internet Directory authenticator:

`ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/config/config.xml`

1. Begin by backing up these relevant configuration files:

```
ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
/config/config.xml
```

```
ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
/config/fmwconfig/jps-config.xml
```

```
ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
/config/fmwconfig/system-jazn-data.xml
```

2. Back up the `ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/servers/adminServer/boot.properties` file for the Administrator Server.
3. Follow these steps to configure the Identity Store to use LDAP, setting the proper authenticator using the WebLogic Administration Server Console:
 - a. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
 - b. Click the **Security Realms** link on the left navigational bar.
 - c. Click the **myrealm** default realm entry to configure it.
 - d. Click the **Providers** tab within the realm.
 - e. Note that there is a DefaultAuthenticator provider configured for the realm.
 - f. Click the **New** button to add a new provider.
 - g. Enter a name for the provider, such as "OIDAuthenticator" for a provider that will authenticate the user to the Oracle Internet Directory.
 - h. Select the "OracleInternetDirectoryAuthenticator" type from the list of authenticators.

- i. Click **OK**.
- j. On the Providers screen, click the newly created OIDAAuthenticator.
- k. Set the Control Flag to **SUFFICIENT**. This indicates that if a user can be authenticated successfully by this authenticator, then it should accept that authentication and should not continue to invoke any additional authenticators. If the authentication fails, it will fall through to the next authenticator in the chain. Make sure all subsequent authenticators also have their control flag set to **SUFFICIENT** also. In particular, check the DefaultAuthenticator and set that to **SUFFICIENT**.
- l. Click **Save** to save this setting.
- m. Click the **Provider Specific** tab to enter the details for the LDAP server.
- n. Enter the details specific to your LDAP server, as shown in the following table:

Parameter	Value	Description
Host		The LDAP server's server ID. For example: oid.mycompany.com
Port		The LDAP server's port number. For example: 636
Principal		The LDAP user DN used to connect to the LDAP server. For example: cn=orcladmin
Credential		The password used to connect to the LDAP server
SSL Enabled	Checked	Specifies whether SSL protocol is used when connecting to LDAP server.
User Base DN		Specify the DN under which your Users start. For example: cn=users, dc=mycompany, dc=com
Group Base DN		Specify the DN that points to your Groups node. For example: cn=groups, dc=mycompany, dc=com
Use Retrieved User Name as Principal	Checked	Must be turned on.

Click **Save** when done.

- o. Click **Activate Changes** to propagate the changes.
- p. The console displays a message that a restart is required for the changes to take effect. Do not restart the servers as indicated; this will be done after setting up all the WebLogic Authenticators, as described in [Section 19.2.4.4, "Stopping and Starting the WebLogic Administration Servers and Managed Servers."](#)

19.2.4.2 Setting Up the Oracle Access Manager Identity Asserter

Follow these steps to set up the OAM ID Asserter:

1. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
2. Navigate to **SecurityRealms > Default Realm Name > Providers**.
3. Click **New** and select **OAMIdentityAsserter** from the drop down menu.
4. Name the asserter, for example: OAMIDAsserter

Then click **OK**.

5. Click the newly-added asserter to see the configuration screen for OAM Identity Asserter.
6. Set the Control Flag to **REQUIRED**, and then click **Save**.
7. Configure the additional attributes below for the OAM Identity Asserter on the **Provider Specific** tab:
 - **Application Domain:** Provide the Oracle Access Manager policy domain name. Use the `app_domain` parameter passed to the OAM Configuration Tool. For example: `IDMEDG`.
 - **Primary Access Server:** Provide Oracle Access Manager server endpoint information in the `host:port` format. For example:
`oamhost1.mycompany.com:6023`
 - **AccessGate Name:** Name of the AccessGate (for example, `IDMEDG_WD`). Provide the AccessGate name created by the OAM Configuration Tool.
 - **AccessGate Password:** Password for the AccessGate, if one was provided.

Accept the default values for all the other attributes, unless required for your environment.
8. Save the settings.
9. Click **Activate Changes** to propagate the changes.

19.2.4.3 Reordering Oracle Access Manager Identity Asserter, Oracle Internet Directory Authenticator, and Default Authenticator

Follow the steps below to reorder the providers in the order shown below:

1. Log into the WebLogic Administration Server Console and click **Lock and Edit** to enable editing.
2. Navigate to **SecurityRealms > Default Realm Name > Providers**.
3. Ensure that the Control Flag for each authenticator is set correctly.
4. Click **Reorder** under the **Authentication Providers** table.
5. On the Reorder Authentication Providers page, reorder the providers as shown below:


```
OAM Identity Asserter (REQUIRED) > OID Authenticator (SUFFICIENT) >
Default Authenticator (SUFFICIENT) > DefaultIdentityAsserter
```
6. Save the settings.
7. Click **Activate Changes** to propagate the changes.

19.2.4.4 Stopping and Starting the WebLogic Administration Servers and Managed Servers

The WebLogic Administration Server and the associated Managed Servers must be restarted for the configuration changes to take effect. Follow the steps below to stop and then start the WebLogic Administration Server and the Managed Servers (`wls_ods1` and `wls_ods2`):

1. Stop the Administration Server and the `wls_ods1` and `wls_ods2` managed servers as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

2. Verify that the server processes have been successfully stopped.
3. On `IDMHOST1`, start the WebLogic Administration Server using the `startWebLogic.sh` script located under the `ORACLE_BASE/admin/IDMDomain/aserver/IDMDomainStatus/bin` directory using the syntax below. This enables the standard output log messages shown on the screen to be written to the file specified in the `logfile` parameter.

```
./startWebLogic.sh >logfile 2>&1 &
```

For example:

```
./startWebLogic.sh > \  
/admin/IDMDomain/aserver/IDMDomainStatus/servers/AdminServer/logs/aserver.out\  
2>&1 &
```

4. Verify that the Administration Server has started up and then bring up the Administration Console using a web browser.
5. Log into the console using the `administrator` user's credentials.
6. Start the `wls_ods1` and `wls_ods2` Managed Servers using the WebLogic Administration Console, as described in [Section 18.1, "Starting and Stopping Oracle Identity Management Components."](#)

19.2.5 Validating the Oracle Access Manager Single Sign-On Setup

To validate the setup, open a web browser and go the following URLs:

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

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

The Oracle Access Manager Single Sign-On page displays. Provide the credentials for the `weblogic_idm` user to log in.

19.3 Configuring Single Sign-on for Administration Consoles with Oracle Access Manager 11g

Numerics

10g Oracle Single Sign-on, 10-2

A

Access Manager

See Oracle Access Manager

Access SDK

defined, 10-1, 11-1

Access Server

assigning to WebGate, 10-40

creating an instance, 10-30

defined, 10-1, 11-1

installing, 10-30, 10-32

AccessGate

defined, 10-1, 11-1

validating the configuration, 19-7

Admin role

assigning to the Admin group, 19-3

Admin users and groups

provisioning in an LDAP directory, 19-2

admin.mycompany.com virtual server, 2-4

application tier

backing up the configuration, 9-12

scaling out, 18-18

scaling up, 18-9

auditing

introduction, 17-34

auditing Identity Management, 17-34

authenticator

setting the Control Flag, 19-9

setting up for OAM ID Asserter, 19-8

setting up for Oracle Internet Directory, 19-7

setting up for WebLogic Server, 19-7

Authorization Policy Manager

configuring, 14-2

auto-login for Oracle Identity Manager

configuring, 17-15

B

backing up Fusion Middleware home, 4-23

backing up installation, 6-13

backup

of runtime artifacts, 18-30

of static artifacts, 18-29

of the application tier configuration, 9-12

of the Oracle Access Manager

configuration, 10-44

backup and recovery, 18-29

boot.properties file

creating, 6-5

updating on IDMHOST1 and IDMHOST2, 19-3

C

certificates

host name verification, 16-3

self-signed, 16-3

component

patching, 18-31

configuration

custom keystores for Node Manager, 16-5

Node Manager, 16-1

Configuration Wizard

creating domain with, 6-2

configuring

admin.mycompany.com virtual server, 2-4

firewall, 2-5

Identity Server, 10-16

oid.mycompany.com virtual server, 2-3

Oracle Access Manager, 10-1, 11-1

ovd.mycompany.com virtual server, 2-4

Policy Manager with Oracle Internet
Directory, 10-25

ports for load balancer, 2-3

sso.mycompany.com virtual server, 2-4

the first Identity Server using WebPass, 10-16

the second Identity Server using WebPass, 10-20

virtual server names on load balancer, 2-3

configuring HTTP server with load balancer, 5-3

Configuring Oracle Access Manager with Web
Tier, 13-17

configuring Oracle Adaptive Access Manager, 12-3

configuring Oracle Adaptive Access Manager with
HTTP server, 12-11

configuring Oracle Internet Directory instances, 7-2

configuring Web Tier, 5-1

connection

component and firewall timeout values, 2-5

creating a domain, 6-1

credential store
 migration, 17-1
 reassociating with Oracle Internet Directory, 17-2
custom keystores, 16-5, 16-6

D

database
 adding a service, 3-4
 configuring for Oracle Fusion Middleware metadata, 3-3
 connections, timeout and, 2-5
 CREATE_SERVICE subprogram, 3-4
 creating services, 3-4
 starting a service, 3-4
deployment
 managing, 18-1
Directory Integration Platform
 installing, 9-4
directory structure
 recommendations, 2-9
 terminology, 2-8
directory tier
 scaling out, 18-17
 scaling up, 18-8
disabling host name verification, 6-7
DNS, virtual server names and, 2-4
DOMAIN directory
 defined, 2-9

E

enterprise deployment
 hardware requirements, 2-1
 high availability, 1-4
 other recommendations, 18-39
 patching, 18-31
 port assignment, 2-5
 ports used, 2-6
 scaling, 18-8
 scaling out, 18-17
 scaling up, 18-8
 security, 1-3
enterprise deployment, defined, 1-1
enterprise topologies, 1-4
etc/services file, 9-2

F

file
 etc/services, 9-2
firewall
 configuring, 2-5
 dropped connections and, 2-5
form authentication
 updating for delegated administration, 19-5
Fusion Middleware components
 installing, 4-6
Fusion Middleware home
 backing up, 4-23
 installing, 4-6

G

GCC 3.3.2 runtime libraries, 10-3
generating self-signed certificates, 16-3
grid servers, 1-1

H

high availability practices, Oracle site, 1-1
host name verification
 certificates for Node Manager, 16-3
 disabling, 6-7
 managed servers, 16-7
host name verification certificates, 16-3
HTTP server
 configuring for WebLogic Administration Server, 6-8
 configuring with APM, 14-4
 installing, 4-4
 registering with WebLogic Server, 6-9

I

identity keystore, 16-4
Identity Management Components
 stopping and starting, 18-1
Identity Server
 configuring, 10-5, 10-8, 10-16
 configuring the first using WebPass, 10-16
 configuring the second using WebPass, 10-20
 defined, 10-1, 11-1
 installing the first, 10-3
 installing the second, 10-7
 specifying encryption mode, 10-5, 10-8
 validating configuration, 10-20
idmhost-vip.mycompany.com
 virtual IP address for WebLogic Administration Server, 2-4
installation
 software, 4-1
installing
 Access Server, 10-30
 an additional Oracle Directory Integration Platform instance, 9-4
 an additional Oracle Directory Services Manager instance, 9-4
 Oracle Access Manager, 10-1, 11-1
 Oracle HTTP Server, 10-10
 Policy Manager, 10-22
 the first Identity Server, 10-3
 the first Oracle Directory Integration Platform instance, 9-1
 the first Oracle Directory Services Manager instance, 9-1
 the second Identity Server, 10-7
 WebGate, 10-35, 10-40
 WebPass, 10-13
installing Fusion Middleware components, 4-6
installing Fusion Middleware home, 4-6
installing HTTP server, 4-4
installing Oracle Access Manager

, 10-1
installing WebLogic server, 4-7

J

Java component
 defined, 1-3
JPS root
 creating, 17-1
jpsroot
 creating using ldapadd command, 17-1

K

keystores
 custom, 16-5, 16-6
 identity, 16-4
 trust, 16-5
Keytool utility, 16-5
knowledge based authentication questions
 loading, 12-13

L

LDAP
 using multiple stores, 10-2, 11-2
LDAP configuration post-setup script, 13-16
LDAP configuration pre-setup script, 13-6
LDAP directory
 creating WebLogic administrative users, 19-1
 provisioning Admin users and groups, 19-2
ldapadd command
 creating the jpsroot in Oracle Internet
 Directory, 17-1
libgcc_s.so.1, 10-2, 10-3
libstdc++.so.5, 10-2, 10-3
listen address
 setting for a Managed Server, 9-7
load balancer
 configuring HTTP server with, 5-3
 configuring ports, 2-3
 configuring virtual server names, 2-3
 required features, 2-2
log file for Node Manager, 16-2

M

Managed Server
 setting listen address for wls_ods1, 9-7
managed servers
 custom keystores, 16-6
 host name verification, 16-7
 provisioning, 9-8
managing deployment, 18-1
monitoring
 Oracle Directory Integration Platform, 18-7
 Oracle Internet Directory, 18-5
 Oracle Virtual Directory, 18-6
MW_HOME
 defined, 2-9

N

Node Manager, 16-3
 custom keystores, 16-5
 described, 16-1
 host name verification certificates, 16-3
 identity keystore, 16-4
 log file, 16-2
 setup, 16-1
 starting, 16-8
 trust keystore, 16-5
Node Manager properties file, 16-2
node manager property file, 12-9

O

OAM Configuration tool
 about, 10-35
 information to collect for, 10-35
 optional parameters and values for CREATE
 mode, 10-37
 parameters and values, 10-36
 running, 10-36
 running in VALIDATE mode, 10-38
 sample command, 10-38
OAM ID Asserter
 setting up authenticator, 19-8
ODSM
 configuring, 9-1
 installing, 9-4
oid.mycompany.com virtual server, 2-3
Oracle Access Manager
 configuring with Web Tier, 11-6
 defined, 10-1, 11-1
 installation prerequisites, 10-2
 installing, 10-1
 Oracle Access Protocol (OAP), 2-5
 Oracle Identity Protocol (OIP), 2-5
 overview of user access requests, 2-5
 scaling out, 18-19
 scaling up, 18-10
 troubleshooting, 18-38
 validating, 10-44
 workaround for installation hang, 10-3
Oracle Access Manager 10g
 integrating with Oracle Identity Manager, 17-11
Oracle Access Manager 11g
 installing, 11-1
 integrating with Oracle Identity Manager, 17-17
Oracle Access Manager identity asserter
 creating, 17-11
Oracle Access Protocol (OAP), 2-5
Oracle Adaptive Access Manager
 configuring, 12-3
 integrating, 17-25
 loading seed data, 12-13
Oracle Adaptive Access Manger
 described, 12-1
Oracle Delegated Administration Service, 10-2
Oracle Directory Integration Platform
 configuring, 9-1

- configuring the first instance, 9-1
- configuring the second instance, 9-4
- copying from one host to another, 9-7
- installing the first instance, 9-1
- installing the second instance, 9-4
- monitoring, 18-7
- post-installation steps, 9-6
- scaling out, 18-18
- scaling up, 18-10
- troubleshooting, 18-33
- validating, 9-10
- Oracle Directory Services Manager
 - configuring the first instance, 9-1
 - configuring the second instance, 9-4
 - installing the first instance, 9-1
 - installing the second instance, 9-4
 - post-installation steps, 9-6
 - scaling out, 18-18
 - scaling up, 18-10
 - troubleshooting, 18-34
 - validating, 9-9
- Oracle Enterprise Manager
 - monitoring Oracle Directory Integration Platform, 18-7
 - monitoring Oracle Internet Directory, 18-5
 - monitoring Oracle Virtual Directory, 18-6
- Oracle Enterprise Manager Fusion Middleware Control
 - defined, 1-3
- Oracle Fusion Middleware Audit Framework
 - introduction, 17-34
- Oracle Fusion Middleware enterprise deployment
 - functions, 1-1
- Oracle Fusion Middleware farm
 - defined, 1-3
- Oracle Fusion Middleware home
 - defined, 1-2
- Oracle home
 - defined, 1-2
- Oracle homes
 - upgrading release, 4-12
- Oracle HTTP Server
 - installing, 10-10
 - validating, 10-12
- Oracle Identity Federation
 - configuring, 15-2
 - described, 15-1
- Oracle Identity Manager
 - configuring, 13-2
 - defined, 13-1
 - integrating with Oracle Access Manager, 17-11
 - integrating with Oracle Access Manager 11g, 17-17
- Oracle Identity Navigator
 - configuring, 14-5
 - described, 14-5
- Oracle Identity Protocol (OIP), 2-5
- Oracle instance
 - defined, 1-2
- Oracle Internet Directory

- component names assigned by installer, 18-6
 - monitoring, 18-5
 - scaling out, 18-18
 - scaling up, 18-8
 - setting up authenticator, 19-7
 - troubleshooting, 18-32
- Oracle Internet Directory instances
 - configuring, 7-2
- Oracle Single Sign-On, 10-2
- Oracle Virtual Directory
 - monitoring, 18-6
 - scaling out, 18-18
 - scaling up, 18-9
 - troubleshooting, 18-33
 - using as identity store, 10-2, 11-2
- Oracle Virtual Directory adapter for Oracle Internet Directory, 9-11
- Oracle WebLogic Administration Server
 - See WebLogic Administration Server
- Oracle WebLogic Server Clusters
 - See WebLogic Server Clusters
- Oracle WebLogic Server domain
 - See WebLogic Server domain
- Oracle WebLogic Server home
 - See WebLogic Server home
- ORACLE_BASE
 - defined, 2-8
- ORACLE_HOME
 - defined, 2-9
- ORACLE_INSTANCE
 - defined, 2-9
- ovd.mycompany.com virtual server, 2-4

P

- patching
 - of a component, 18-31
 - of a source file, 18-31
 - of an enterprise deployment, 18-31
- performance, enterprise deployment and, 1-1
- persistence store, 13-19
- policy domain
 - validating the configuration, 19-6
- Policy Manager
 - configuring with Oracle Internet Directory, 10-25
 - defined, 10-1, 11-1
 - installing, 10-22
- policy store
 - migration, 17-1
 - reassociating with Oracle Internet Directory, 17-2
- pooled connections, timeout and, 2-5
- port
 - freeing, 9-2
- port assignment, 2-5
- ports
 - configuring for load balancer, 2-3
 - used in enterprise deployment, 2-6
- providers
 - reordering, 19-9
- provisioning managed servers, 9-8

R

- RCU, 3-5
 - creating Identity Management schemas, 3-5
 - executing, 3-5
- registering Oracle Internet Directory with WebLogic Server domain, 7-7
- registering Oracle Virtual Directory with WebLogic Server domain, 8-5
- Repository Creation Utility, 3-5
 - See RCU, 3-5
- Request Cache type
 - changing, 11-8

S

- scaling
 - of enterprise deployments, 18-8
- scaling out
 - application tier, 18-18
 - directory tier, 18-17
 - enterprise deployment, 18-17
 - Oracle Access Manager, 18-19
 - Oracle Directory Integration Platform, 18-18
 - Oracle Directory Services Manager, 18-18
 - Oracle Internet Directory, 18-18
 - Oracle Virtual Directory, 18-18
 - web tier, 18-29
- scaling up
 - application tier, 18-9
 - directory tier, 18-8
 - enterprise deployment, 18-8
 - Oracle Access Manager, 18-10
 - Oracle Directory Integration Platform, 18-10
 - Oracle Directory Services Manager, 18-10
 - Oracle Internet Directory, 18-8
 - Oracle Virtual Directory, 18-9
 - web tier, 18-17
- self-signed certificates, 16-3
- service
 - assigning to an instance, 3-4
- service level agreements, 1-1
- setting up Node Manager, 16-1
- shared JMS persistence store, 13-19
- Single Sign-On
 - prerequisites, 19-5
- Single Sign-on
 - 10g, 10-2
 - configuring for administration consoles, 19-1
 - configuring for administration consoles using OAM 11g, 19-10
 - Single Sign-on 11g
 - integrating administration consoles, 17-9
 - Single Sign-On for Oracle Access Manager
 - validating, 19-10
- SOA
 - upgrading release, 4-12
- software installation, 4-1
- software versions, 4-4
- source file
 - patching, 18-31

- SSL port, LDAP and Oracle Internet Directory, 2-3
- sso.mycompany.com virtual server, 2-4
- starting
 - Node Manager, 16-8
- system component
 - defined, 1-3

T

- TAF settings, 3-4
- terminology
 - directory structure, 2-8
 - DOMAIN directory, 2-9
 - MW_HOME, 2-9
 - ORACLE_BASE, 2-8
 - ORACLE_HOME, 2-9
 - ORACLE_INSTANCE, 2-9
 - WL_HOME, 2-9
- timeout
 - values, Oracle Fusion Middleware components and firewall/load balancer, 2-5
- timeouts for SQL*Net connections
 - preventing, 18-39
- topologies
 - enterprise, 1-4
- topology
 - building, 1-26
- Topology 1 - Oracle Access Manager 11g, 1-4
- Topology 2 - Oracle Access Manager 10g and Oracle Identity Manager 11g, 1-8
- Topology 3 - Oracle Access Manager 11g and Oracle Identity Manager 11g, 1-13
- Topology 4 - Oracle Adaptive Access Manager 11g, 1-17
- Topology 5 - Oracle Identity Federation 11g, 1-21
- Transparent Application Failover settings, 3-4
- troubleshooting
 - Oracle Access Manager, 18-38
 - Oracle Directory Integration Platform, 18-33
 - Oracle Directory Services Manager, 18-34
 - Oracle Internet Directory, 18-32
 - Oracle Virtual Directory, 18-33
 - redirection to WebLogic Server Administration Console Home page, 18-39
 - redirection to WebLogic Server Administration Console login screen, 18-38
- trust keystore, 16-5

U

- upgrading existing topology, 4-23
- upgrading release
 - Oracle homes and SOA, 4-12
- utils.CertGen utility, 16-3
- utils.ImportPrivateKey utility, 16-4

V

- validating
 - AccessGate configuration, 19-6
 - Oracle Access Manager Single Sign-On, 19-10

- Oracle HTTP Server, 10-12
 - policy domain configuration, 19-6
 - the AccessGate configuration, 19-7
 - WebPass, 10-16
- versions
 - software, 4-4
- virtual IP address, 2-4
 - associating weblogic Administration Server, 6-2
 - configuring for WebLogic Administration Server, 2-4
- virtual server
 - configuring admin.mycompany.com, 2-4
 - configuring oid.mycompany.com, 2-3
 - configuring ovd.mycompany.com, 2-4
 - configuring sso.mycompany.com, 2-4

W

- Web Tier
 - configuring, 5-1
- web tier
 - scaling out, 18-29
 - scaling up, 18-17
- WebGate
 - configuring, 17-3
 - defined, 10-1, 11-1
 - installing, 10-35, 10-40, 17-3
- WebGate agent
 - creating, 17-3
- WebLogic Administration Server
 - associating with virtual IP address, 6-2
 - configuring virtual IP address for, 2-4
 - failing over, 6-10
- WebLogic administrative users
 - creating in an LDAP directory, 19-1
- WebLogic Server
 - setting up authenticator, 19-7
- WebLogic server
 - installing, 4-7
- WebLogic Server Domain
 - creating, 6-1
- WebLogic Server domain
 - considerations, 2-8
 - defined, 1-3
 - registering Oracle Internet Directory, 7-7
 - registering Oracle Virtual Directory, 8-5
- WebLogic Server home
 - defined, 1-2
- WebPass
 - defined, 10-1, 11-1
 - installing, 10-13
 - validating, 10-16
- WL_HOME
 - defined, 2-9