

Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle WebCenter Portal

11g Release 1 (11.1.1.6.0)

E12037-06

December 2011

Documentation for installers that describes how to install and configure Oracle WebCenter Portal components in an enterprise deployment. Includes best practices blueprint for an Oracle WebCenter Portal enterprise deployment topology.

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Portal, 11g Release 1
(11.1.1.6.0)

E12037-06

Copyright © 2009, 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Rosie Harvey

Contributing Author: Richard Delval,

Contributor: Janga Aliminati, Fermin Castro Alonso, Pradeep Bhat, Martin Fry, Roy Sandjaja

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 is software or related documentation that 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 or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware 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	xi
Audience	xi
Documentation Accessibility	xi
Related Documents	xi
Conventions	xii
1 Enterprise Deployment Overview	
1.1 About the Enterprise Deployment Guide	1-1
1.2 Enterprise Deployment Terminology	1-2
1.3 Benefits of Oracle Recommendations	1-5
1.3.1 Built-in Security	1-5
1.3.2 High Availability	1-6
2 Introduction to the Enterprise Deployment Reference Topology	
2.1 Overview of Enterprise Deployment Reference Topology	2-1
2.1.1 Reference Topology Documented in the Guide	2-1
2.1.2 About Oracle Identity Management Integration	2-2
2.1.3 About the Web Tier Nodes	2-3
2.1.3.1 Load Balancer Requirements	2-3
2.1.4 About the Application Tier	2-4
2.1.5 About the Data Tier	2-5
2.1.6 About the Unicast Requirement for Communication	2-5
2.2 Hardware Requirements for an Enterprise Deployment on Linux	2-6
2.3 Clock Synchronization	2-6
2.4 Identifying the Software Components to Install	2-6
2.5 Road Map for the Reference Topology Installation and Configuration	2-7
2.5.1 Flow Chart of the Oracle WebCenter Portal Enterprise Deployment Process	2-7
2.5.2 Steps in the Oracle WebCenter Portal Enterprise Deployment Process	2-8
2.5.3 Understanding the Incremental, Modular Approach to Enterprise Deployment ..	2-10
3 Preparing the Network for an Enterprise Deployment	
3.1 Overview of Preparing the Network for an Enterprise Deployment	3-1
3.2 About Virtual Server Names Used by the Topology	3-1
3.2.1 wcp.mycompany.com	3-2
3.2.2 admin.mycompany.com	3-2

3.2.3	wcpinternal.mycompany.com	3-2
3.3	Configuring the Load Balancer	3-2
3.4	About IPs and Virtual IPs	3-4
3.5	About Firewalls and Ports	3-5
3.6	About LDAP as Credential and Policy Store	3-8
4	Preparing the File System for an Enterprise Deployment	
4.1	Overview of Preparing the File System for Enterprise Deployment	4-1
4.2	Terminology for Directories and Directory Environment Variables	4-1
4.3	About Recommended Locations for the Different Directories.....	4-2
4.4	Configuring Shared Storage	4-10
5	Preparing the Database for an Enterprise Deployment	
5.1	Overview of Preparing the Database for an Enterprise Deployment	5-1
5.2	About Database Requirements	5-1
5.2.1	Database Host Requirements.....	5-2
5.2.2	Supported Database Versions.....	5-2
5.2.3	About Initialization Parameters	5-2
5.3	Creating Database Services	5-3
5.4	Loading the Oracle Fusion Metadata Repository in the Oracle RAC Database	5-4
5.5	Configuring SOA Schemas for Transactional Recovery Privileges.....	5-6
5.6	Backing Up the Database	5-6
6	Installing the Software for an Enterprise Deployment	
6.1	Overview of the Software Installation Process.....	6-1
6.2	Installing Oracle HTTP Server	6-2
6.2.1	Prerequisites to Installing Oracle HTTP Server	6-2
6.2.2	Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2.....	6-2
6.2.3	Backing Up the Oracle Fusion Middleware Installation.....	6-3
6.3	Installing Oracle Fusion Middleware	6-3
6.3.1	Installing Oracle WebLogic Server and Creating the Fusion Middleware Home	6-4
6.3.2	Installing Oracle Fusion Middleware Components.....	6-5
6.3.2.1	Installing Oracle SOA Suite.....	6-5
6.3.2.2	Installing Oracle WebCenter Portal	6-7
6.3.2.3	Installing Oracle WebCenter Content.....	6-8
6.3.3	Backing Up the Fusion Middleware Installation	6-9
7	Configuring the Web Tier for an Enterprise Deployment	
7.1	Overview of Configuring the Web Tier.....	7-1
7.2	Running the Configuration Wizard to Configure Oracle HTTP Server	7-1
7.3	Validating the Oracle HTTP Server Configuration.....	7-3
7.4	Associating the Oracle Web Tier with the Oracle WebLogic Domain	7-3
7.5	Configuring the Load Balancer to Route HTTP Requests	7-3
7.6	Configuring Virtual Hosts	7-3
7.6.1	Editing the httpd.conf File.....	7-3
7.6.2	Restarting Both OHS Servers	7-4

7.6.3	Validating the Configuration	7-4
-------	------------------------------------	-----

8 Creating a Domain for an Enterprise Deployment

8.1	Overview of Creating a Domain.....	8-1
8.2	Enabling VIP1 in SOAHOST1	8-2
8.3	Running the Configuration Wizard on SOAHOST1 to Create a Domain	8-3
8.4	Post-Configuration and Verification Tasks	8-7
8.4.1	Creating boot.properties for the Administration Server on SOAHOST1.....	8-8
8.4.2	Starting Node Manager on SOAHOST1.....	8-8
8.4.3	Starting the Administration Server on SOAHOST1	8-9
8.4.4	Validating the Administration Server Configuration	8-10
8.4.5	Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server	8-10
8.4.6	Applying the Java Required Files (JRF) Template to the WSM-PM_Cluster.....	8-11
8.4.7	Disabling Host Name Verification for the Administration Server and the WLS_WSM1 Managed Server	8-11
8.4.8	Starting and Validating the WLS_WSM1 Managed Server.....	8-12
8.5	Propagating the Domain Configuration to SOAHOST2	8-12
8.5.1	Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility	8-13
8.5.2	Disabling Host Name Verification for the WLS_WSM2 Managed Server	8-13
8.5.3	Starting Node Manager on SOAHOST2.....	8-14
8.5.4	Starting and Validating the WLS_WSM2 Managed Server.....	8-14
8.5.5	Configuring the Java Object Cache for Oracle WSM.....	8-14
8.6	Configuring Oracle HTTP Server for the WebLogic Domain	8-16
8.6.1	Configuring Oracle HTTP Server for the Administration Server and the WLS_WSM <i>n</i> Managed Servers	8-16
8.6.2	Turning on the WebLogic Plug-In Enabled Flag	8-18
8.6.3	Registering Oracle HTTP Server With WebLogic Server	8-19
8.6.4	Setting the Frontend URL for the Administration Console and Setting Redirection Preferences	8-19
8.6.5	Validating Access Through Oracle HTTP Server.....	8-20
8.6.6	Manually Failing Over the Administration Server to SOAHOST2.....	8-20
8.6.7	Validating Access to SOAHOST2 Through Oracle HTTP Server.....	8-22
8.6.8	Failing the Administration Server Back to SOAHOST1	8-22
8.7	Backing Up the WebLogic Domain Configuration.....	8-23

9 Extending the Domain for SOA Components

9.1	Overview of Extending the Domain for SOA Components	9-1
9.2	Preparing to Extend the Domain for Oracle SOA Components	9-2
9.2.1	Enabling VIP2 on SOAHOST1 and VIP3 on SOAHOST2.....	9-2
9.3	Extending the Domain for SOA Components using the Configuration Wizard.....	9-3
9.4	Configuring Oracle Coherence for Deploying Composites.....	9-8
9.4.1	Enabling Communication for Deployment Using Unicast Communication.....	9-8
9.4.2	Specifying the Host Name Used by Oracle Coherence.....	9-9
9.5	Post-Configuration and Verification Tasks	9-11
9.5.1	Disabling Host Name Verification for the WLS_SOA <i>n</i> Managed Server	9-11
9.5.2	Restarting the Node Manager on SOAHOST1	9-12

9.5.3	Propagating the Domain Changes to the Managed Server Domain Directory	9-12
9.5.4	Starting and Validating the WLS_SOA1 Managed Server	9-13
9.6	Propagating the Domain Configuration to SOAHOST2	9-13
9.6.1	Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility	9-14
9.6.2	Starting and Validating the WLS_SOA2 Managed Server	9-14
9.7	Configuring Oracle HTTP Server with the Extended Domain	9-15
9.7.1	Configuring Oracle HTTP Server for the WLS_SOA n Managed Servers	9-15
9.7.2	Validating Access Through Oracle HTTP Server.....	9-17
9.7.3	Setting the Frontend HTTP Host and Port.....	9-17
9.8	Configuring a Default Persistence Store for Transaction Recovery	9-19
9.9	Configuring Oracle Adapters.....	9-20
9.9.1	Enabling High Availability for Oracle File and FTP Adapters	9-20
9.9.1.1	Using the Database Mutex Locking Operation.....	9-20
9.9.2	Enabling High Availability for Oracle JMS Adapter.....	9-23
9.9.3	Scaling the Oracle Database Adapter	9-23
9.10	Backing Up the SOA Configuration.....	9-24

10 Extending the Domain for WebCenter Portal Components

10.1	Overview of Extending the Domain for WebCenter Portal Components.....	10-1
10.2	Extending the Domain for WebCenter Portal Components using the Configuration Wizard	10-2
10.3	Post-Configuration Tasks	10-7
10.3.1	Disabling Host Name Verification for the WebCenter Portal Managed Servers	10-8
10.3.2	Starting Node Manager on SOAHOST1.....	10-8
10.3.3	Propagating the Domain Changes to the Managed Server Domain Directory	10-9
10.4	Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2.....	10-9
10.4.1	Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2 Using the unpack Utility	10-10
10.4.2	Starting the Node Manager on WCPHOST1 and WCPHOST2	10-10
10.4.3	Starting the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers on WCPHOST1	10-11
10.4.4	Validating the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers	10-11
10.4.5	Starting the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 Managed Servers on WCPHOST2	10-12
10.4.6	Validating the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 Managed Servers	10-12
10.5	Configuring the Java Object Cache for Spaces_Cluster.....	10-13
10.6	Converting Discussions from Multicast to Unicast	10-14
10.7	Configuring Clustering on the Discussions Server.....	10-15
10.8	Configuring Analytics.....	10-16
10.9	Configuring Activity Graph.....	10-16
10.10	Configuring REST APIs	10-17
10.11	Configuring Oracle HTTP Server with the Extended Domain	10-17
10.11.1	Configuring Oracle HTTP Server for the WC_Spaces n , WC_Portlet n , WC_Uilities n , and WC_Collaboration n Managed Servers	10-18
10.11.1.1	Configuring Microsoft Clients.....	10-21

10.11.2	Validating Access Through Oracle HTTP Server.....	10-21
10.11.3	Validating Access Through the Load Balancer	10-22
10.12	Backing Up the WebCenter Portal Configuration.....	10-22

11 Setting Up Node Manager for an Enterprise Deployment

11.1	Overview of the Node Manager	11-1
11.2	Changing the Location of Node Manager Log	11-1
11.3	Enabling Host Name Verification Certificates for Node Manager in SOAHOST1 and WCPHOST1 11-2	
11.3.1	Generating Self-Signed Certificates Using the utils.CertGen Utility	11-2
11.3.2	Creating an Identity Keystore Using the utils.ImportPrivateKey Utility.....	11-3
11.3.3	Creating a Trust Keystore Using the Keytool Utility	11-4
11.3.4	Configuring Node Manager to Use the Custom Keystores.....	11-5
11.3.5	Using a Common or Shared Storage Installation.....	11-5
11.4	Starting the Node Manager on SOAHOST1	11-5
11.5	Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2 11-6	
11.5.1	Generating Self-Signed Certificates Using the utils.CertGen Utility	11-6
11.5.2	Creating an Identity Keystore in Using the utils.ImportPrivateKey Utility	11-7
11.5.3	Configuring Node Manager to Use the Custom Keystores.....	11-8
11.6	Starting Node Manager on SOAHOST2.....	11-8
11.7	Configuring WebLogic Servers to Use the Custom Keystores.....	11-9

12 Configuring External WebCenter Portal Services for an Enterprise Deployment

12.1	Configuring the Discussions Server Connection.....	12-1
12.1.1	Creating a Discussions Server Connection Using Fusion Middleware Control	12-2
12.1.2	Creating a Discussions Server Connection using WLST	12-2
12.2	Configuring the Instant Messaging and Presence (IMP) Server Connection.....	12-3
12.3	Configuring a BPEL Server Connection for Worklists and Workflows.....	12-3
12.3.1	Before You Start	12-3
12.3.2	Configuring Worklists and Workflow using Fusion Middleware Control.....	12-3
12.3.3	Configuring Worklist and Workflow using WLST.....	12-4
12.4	Registering Portlet Producers	12-5
12.4.1	Registering Out-of-the-Box Portlet Producers using Fusion Middleware Control	12-5
12.4.2	Registering Out-of-the-Box Portlet Producers Using WLST	12-5
12.5	Registering the Pagelet Producer	12-6
12.6	Configuring Search Services	12-6
12.7	Configuring the Mail Server for Notifications.....	12-7

13 Extending the Domain to Include Oracle WebCenter Content

13.1	Overview of Extending the Domain to Include Oracle WebCenter Content.....	13-2
13.2	Extending the Domain to Include Oracle WebCenter Content.....	13-3
13.3	Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility 13-7	
13.4	Configuring the Load Balancer to Route WebCenter Content Traffic	13-8

13.5	Starting Node Manager on WCPHOST1 and WCPHOST2.....	13-9
13.6	Restarting the Administration Server	13-9
13.7	Starting and Configuring the WLS_WCC1 Managed Server	13-9
13.8	Updating the cwallet File in the Administration Server	13-11
13.9	Starting and Configuring the WLS_WCC2 Managed Server	13-11
13.10	Configuring Service Retries for Oracle WebCenter Content.....	13-12
13.11	Configuring Oracle HTTP Server for the WLS_WCC Managed Servers.....	13-13
13.12	Validating Access Through Oracle HTTP Server.....	13-14
13.13	Backing Up the Installation	13-14
13.14	Configure Oracle WebCenter Content for Oracle WebCenter Portal	13-15
13.14.1	Enabling Mandatory Content Server Components (Folders_g and WebCenterConfigure) 13-15	
13.14.2	Enabling and Configuring the Dynamic Converter Component	13-16
13.14.3	Configuring Additional Content Server Features.....	13-16
13.15	Registering Oracle WebCenter Content with Oracle WebCenter Portal Applications	13-16
13.16	Installing and Configuring the Inbound Refinery	13-18
13.16.1	Extending the Domain to Include Inbound Refinery	13-18
13.16.2	Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility 13-20	
13.16.3	Restarting the Administration Server	13-21
13.16.4	Starting the Inbound Refinery Managed Servers.....	13-21
13.16.5	Configuring Inbound Refinery	13-21
13.16.5.1	Configuring Inbound Refinery Settings.....	13-22
13.16.5.2	Configuring Document Conversion	13-23
13.16.5.3	Configuring Oracle WebCenter Content with the Inbound Refinery	13-24

14 Configuring Server Migration for an Enterprise Deployment

14.1	Overview of Server Migration for an Enterprise Deployment	14-1
14.2	Setting Up a User and Tablespace for the Server Migration Leasing Table.....	14-1
14.3	Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console.. 14-2	
14.4	Enabling Host Name Verification Certificates between SOAHOST1 and SOAHOST2 and the Administration Server 14-3	
14.5	Editing the Node Manager's Properties File.....	14-4
14.6	Setting Environment and Superuser Privileges for the wlsifconfig.sh Script.....	14-5
14.7	Configuring Server Migration Targets	14-5
14.8	Testing Server Migration	14-6

15 Integrating an Enterprise Deployment with Oracle Identity Management

15.1	Overview of Integration With Oracle Identity Management	15-1
15.2	Configuring the Credential Store	15-3
15.2.1	Creating the LDAP Authenticator.....	15-4
15.2.2	Moving the WebLogic Administrator to LDAP	15-5
15.2.2.1	Provisioning Admin Users and Groups in an LDAP Directory	15-6
15.2.2.2	Assigning the Admin Role to the Admin Group.....	15-7
15.2.2.3	Updating the boot.properties File and Restarting the System.....	15-8
15.2.3	Reassociating the Domain Credential Store.....	15-8

15.3	Configuring the Policy Store	15-8
15.3.1	Setting a Node in the Server Directory	15-9
15.3.2	Reassociating the Domain Policy Store	15-10
15.4	Reassociating Credentials and Policies	15-10
15.5	Oracle Access Manager 10g Integration	15-11
15.5.1	Overview of Oracle Access Manager Integration	15-12
15.5.2	Prerequisites for Oracle Access Manager	15-12
15.5.3	Using the OAM Configuration Tool	15-13
15.5.3.1	Prerequisites for Running the OAM Configuration Tool	15-13
15.5.3.2	Running the OAM Configuration Tool	15-13
15.5.3.3	Updating the REST Policies	15-16
15.5.3.4	Creating an Exclusion Policy for Oracle SES and Portlets	15-17
15.5.3.5	Verifying Successful Creation of the Policy Domain and AccessGate	15-18
15.5.3.6	Updating the Host Identifier	15-19
15.5.3.7	Updating the WebGate Profile	15-20
15.5.3.8	Adding Additional Access Servers	15-21
15.5.3.9	Configuring Delegated Form Authentication	15-22
15.5.4	Installing and Configuring WebGate	15-22
15.5.5	Configuring IP Validation for the Webgate	15-26
15.5.6	Setting Up WebLogic Authenticators	15-26
15.5.6.1	Back Up Configuration Files	15-27
15.5.6.2	Setting Up the OAM ID Asserter	15-27
15.5.6.3	Setting the Order of Providers	15-27
15.5.7	Configuring Virtual Hosts for OAM 10g	15-28
15.6	Oracle Access Manager 11g Integration	15-29
15.6.1	Overview of Oracle Access Manager Integration	15-29
15.6.2	Prerequisites for Oracle Access Manager	15-30
15.6.3	Installing WebGate	15-30
15.6.3.1	Prerequisite for Installing GCC Libraries	15-30
15.6.3.2	Installing WebGate	15-31
15.6.3.3	Post-Installation Steps	15-32
15.6.4	Registering the WebGate Agent	15-33
15.6.4.1	The RREG Tool	15-33
15.6.4.2	Updating the OAM11gRequest file	15-34
15.6.4.3	Running the oamreg Tool	15-37
15.6.4.4	Copying Access files to WEBHOSTs	15-37
15.6.4.5	Updating REST Policies	15-38
15.6.5	Setting Up the WebLogic Authenticators	15-39
15.6.5.1	Back Up Configuration Files	15-39
15.6.5.2	Setting Up the OAM ID Asserter	15-39
15.6.5.3	Setting the Order of Providers	15-40
15.6.6	Configuring Virtual Hosts for OAM11g	15-40
15.7	Configuring WebCenter Portal Applications for SSO	15-42
15.7.1	Configuring System Properties for WebCenter Portal: Spaces	15-42
15.7.2	Configuring the WebCenter Portal: Spaces Administrator Role	15-42
15.7.2.1	Granting the Spaces Administrator Role Using WLST	15-43
15.7.2.2	Granting the Spaces Administrator Role Using Fusion Middleware Control	15-43

15.7.3	Setting Up Discussions Server to Use OAM as SSO Provider	15-44
15.7.3.1	Granting Administrator Permissions on the Discussions Server	15-44
15.7.3.2	Configuring System Properties for Discussions Server	15-45
15.8	Configuring WebCenter Portal and BPEL Authentication.....	15-45
15.8.1	Verify Authenticators.....	15-45
15.8.2	Set Role Members for BPMWorkflowAdmin Application Role in soa-infra	15-45
15.8.3	Configure SOA Callback URLs.....	15-46
15.9	Backing Up the Identity Management Configuration.....	15-46

16 Managing the Topology for an Enterprise Deployment

16.1	Overview of Managing Monitoring the Topology.....	16-1
16.2	Managing Space in the SOA Infrastructure Database.....	16-2
16.3	Configuring UMS Drivers	16-3
16.4	Scaling Up the Topology (Adding Managed Servers to Existing Nodes)	16-3
16.4.1	Scaling up Oracle SOA (includes WSM)	16-4
16.4.2	Scaling Up WebCenter Portal	16-8
16.5	Scaling Out the Topology (Adding Managed Servers to New Nodes).....	16-9
16.5.1	Scaling out Oracle SOA (includes WSM)	16-9
16.5.2	Scaling Out Oracle WebCenter Portal	16-15
16.6	Performing Backups and Recoveries in WebCenter Portal Deployments	16-17
16.7	Preventing Timeouts for SQLNet Connections	16-18
16.8	Troubleshooting Oracle WebCenter Portal Enterprise Deployments.....	16-19
16.8.1	Error While Activating Changes in Administration Console	16-19
16.8.2	Redirecting of Users to Login Screen After Activating Changes in Administration Console 16-20	
16.8.3	Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM 16-20	
16.8.4	WC_Spaces Server Does Not Start after Propagation of Domain	16-20
16.8.5	Administration Server Fails to Start After a Manual Failover	16-20
16.8.6	Portlet Unavailable After Database Failover	16-21
16.8.7	Configured JOC Port Already in Use	16-21
16.8.8	Restoring a JMS Configuration.....	16-21
16.8.9	OAM Configuration Tool Does Not Remove URLs	16-22
16.8.10	Disabling Secondary Authentication After REST Policy Configuration	16-22
16.8.11	Sudo Error Occurs During Server Migration	16-22

Index

Preface

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

Audience

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

Documentation Accessibility

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

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 architectures:

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

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

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.
<code>monospace</code>	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

This chapter provides an overview of the enterprise topology for Oracle WebCenter Portal. It contains the following sections:

- [Section 1.1, "About the Enterprise Deployment Guide"](#)
- [Section 1.2, "Enterprise Deployment Terminology"](#)
- [Section 1.3, "Benefits of Oracle Recommendations"](#)

1.1 About the Enterprise Deployment Guide

The Enterprise Deployment Guide is an Oracle best practices blueprint based on proven Oracle high-availability and security technologies and recommendations for an Oracle WebCenter Portal enterprise deployment. The best practices described in these blueprints span many Oracle products across the entire technology stack: Oracle Database, Oracle Fusion Middleware, and Enterprise Manager Fusion Middleware 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
- uses Oracle best practices and recommended architecture, which are independent of hardware and operating systems.

For more information on high availability practices, see the Oracle Database High Availability page on Oracle Technology Network at <http://www.oracle.com/technetwork/database/features/availability/index-087701.html>.

Note: The Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Portal focuses on enterprise deployments in Linux environments. However, you can also implement enterprise deployments using UNIX and Windows environments.

1.2 Enterprise Deployment Terminology

This section identifies terms used to describe components in prior releases, and the terms to which they correlate in 11g Release 1 (11.1.1.6.0)

- **Oracle home:** An Oracle home contains installed files necessary to host a specific product. For example, the WebCenter Portal Oracle home contains a directory that contains binary and library files for Oracle WebCenter Portal. An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.
- **Oracle Common home:** This environment variable and related directory path refers to the Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).
- **WebLogic Server home:** A WebLogic Server home contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of Oracle home directories and resides within the directory structure of the Middleware home.
- **Middleware home:** A Middleware home consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
- **Oracle instance:** An Oracle instance contains one or more active middleware system components, for example Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. You determine which components are part of an instance, either at install time or by creating and configuring an instance at a later time. An Oracle instance contains files that can be updated, such as configuration files, log files, temporary files.
- **failover:** When a member of a high availability system fails unexpectedly (unplanned downtime), in order to continue offering services to its consumers, the system undergoes a failover operation. If the system is an active-passive system, the passive member is activated during the failover operation and consumers are directed to it instead of the failed member. The failover process can be performed manually, or it can be automated by setting up hardware cluster services to detect failures and move cluster resources from the failed node to the standby node. If the system is an active-active system, the failover is performed by the load balancer entity serving requests to the active members. If an active member fails, the load balancer detects the failure and automatically redirects requests for the failed member to the surviving active members. See *Oracle Fusion Middleware High Availability Guide* for information on active-active and active-passive systems.
- **failback:** After a system undergoes a successful failover operation, the original failed member can be repaired over time and be re-introduced into the system as a standby member. If desired, a failback process can be initiated to activate this member and deactivate the other. This process reverts the system back to its pre-failure configuration.
- **hardware cluster:** A hardware cluster is a collection of computers that provides a single view of network services (for example: an IP address) or application services (for example: databases, Web servers) to clients of these services. Each node in a hardware cluster is a standalone server that runs its own processes. These processes can communicate with one another to form what looks like a single system that cooperatively provides applications, system resources, and data to users.

A hardware cluster achieves high availability and scalability through the use of specialized hardware (cluster interconnect, shared storage) and software (health monitors, resource monitors). (The cluster interconnect is a private link used by the hardware cluster for heartbeat information to detect node death.) Due to the need for specialized hardware and software, hardware clusters are commonly provided by hardware vendors such as Sun, HP, IBM, and Dell. While the number of nodes that can be configured in a hardware cluster is vendor dependent, for the purpose of Oracle Fusion Middleware high availability, only two nodes are required. Hence, this document assumes a two-node hardware cluster for high availability solutions employing a hardware cluster.

- **cluster agent:** The software that runs on a node member of a hardware cluster that coordinates availability and performance operations with other nodes. Clusterware provides resource grouping, monitoring, and the ability to move services. A cluster agent can automate the service failover.
- **clusterware:** A software that manages the operations of the members of a cluster as a system. It allows one to define a set of resources and services to monitor via a heartbeat mechanism between cluster members and to move these resources and services to a different member in the cluster as efficiently and transparently as possible.
- **shared storage:** Shared storage is the storage subsystem that is accessible by all the machines in the enterprise deployment domain. Among other things, the following are located on the shared disk:
 - Middleware Home software
 - AdminServer Domain Home
 - JMS
 - Tlogs (where applicable)

Managed Server homes can also be optionally located in the shared disk. The shared storage can be a Network Attached Storage (NAS), a Storage Area Network (SAN) or any other storage system that multiple nodes can access simultaneously and can read-write.

- **primary node:** The node that is actively running an Oracle Fusion Middleware instance at any given time and has been configured to have a backup/secondary node. If the primary node fails, Oracle Fusion Middleware instance is failed over to the secondary node. This failover can be manual or automated using the Clusterware for Administration Server. For a server migration based scenario, WebLogic Whole Server Migration is used for automated failover.
- **secondary node:** The node that is the backup node for an Oracle Fusion Middleware instance. This is where the active instance fails over when the primary node is no longer available. See the definition for primary node in this section.
- **network host name:** Network host name is a name assigned to an IP address either through the `/etc/hosts` file or through DNS resolution. This name is visible in the network that the machine to which it refers to is connected. Often, the network host name and physical host name are identical. However, each machine has only one physical host name but may have multiple network host names. Thus, a machine's network host name may not always be its physical host name.
- **physical host name:** This guide differentiates between the terms physical host name and network host name. This guide uses physical host name to refer to the

"internal name" of the current machine. On UNIX, this is the name returned by the `hostname` command.

Physical host name is used by Oracle Fusion Middleware to reference the local host. During installation, the installer automatically retrieves the physical host name from the current machine and stores it in the Oracle Fusion Middleware configuration metadata on disk.

- **physical IP:** Physical IP refers to the IP of a machine on the network. In almost all cases, it is normally associated with the physical host name of the machine (see the definition of the physical host name). In contrast to a virtual IP, it is always associated with the same machine when on a network.
- **switchover:** During normal operation, active members of a system may require maintenance or upgrading. A switchover process can be initiated to allow a substitute member to take over the workload performed by the member that requires maintenance or upgrading, which undergoes planned downtime. The switchover operation ensures continued service to consumers of the system.
- **switchback:** When a switchover operation is performed, a member of the system is deactivated for maintenance or upgrading. When the maintenance or upgrading is completed, the system can undergo a switchback operation to activate the upgraded member and bring the system back to the pre-switchover configuration.
- **virtual host name:** Virtual host name is a network addressable host name that maps to one or more physical machines via a load balancer or a hardware cluster. For load balancers, the name "virtual server name" is used interchangeably with virtual host name in this book. A load balancer can hold a virtual host name on behalf of a set of servers, and clients communicate indirectly with the machines using the virtual host name. A virtual host name in a hardware cluster is a network host name assigned to a cluster virtual IP. Because the cluster virtual IP is not permanently attached to any particular node of a cluster, the virtual host name is not permanently attached to any particular node either.

Note: Whenever the term "virtual host name" is used in this document, it is assumed to be associated with a virtual IP address. In cases where just the IP address is needed or used, it will be explicitly stated.

- **virtual IP:** Also, cluster virtual IP and load balancer virtual IP. Generally, a virtual IP can be assigned to a hardware cluster or load balancer. To present a single system view of a cluster to network clients, a virtual IP serves as an entry point IP address to the group of servers which are members of the cluster. A virtual IP can be assigned to a server load balancer or a hardware cluster.

A hardware cluster uses a cluster virtual IP to present to the outside world the entry point into the cluster (it can also be set up on a standalone machine). The hardware cluster's software manages the movement of this IP address between the two physical nodes of the cluster while clients connect to this IP address without the need to know which physical node this IP address is currently active on. In a typical two-node hardware cluster configuration, each machine has its own physical IP address and physical host name, while there could be several cluster IP addresses. These cluster IP addresses float or migrate between the two nodes. The node with current ownership of a cluster IP address is active for that address.

A load balancer also uses a virtual IP as the entry point to a set of servers. These servers tend to be active at the same time. This virtual IP address is not assigned to

any individual server but to the load balancer which acts as a proxy between servers and their clients.

1.3 Benefits of Oracle Recommendations

The Oracle Fusion Middleware configurations discussed in this guide are designed to ensure security of all invocations, maximize hardware resources, and provide a reliable, standards-compliant system for enterprise computing with a variety of applications.

- [Section 1.3.1, "Built-in Security"](#)
- [Section 1.3.2, "High Availability"](#)

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:

- Configure external load balancers to redirect all external communication received on port 80 to port 443.

Note: The Oracle Technology Network (<http://www.oracle.com/technology/index.html>) provides a list of validated load balancers and their configuration at <http://www.oracle.com/technetwork/middleware/ias/tested-lbr-fw-sslaccel-100648.html>.

- 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 is allowed.
- Components are separated in different protection zones: the web tier, application tier, and the data tier.
- Direct communication across two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory is isolated in the data tier.
- Identity Management components are in a separate subnet.
- All communication between components across protection zones 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.

Introduction to the Enterprise Deployment Reference Topology

This chapter provides an overview of the enterprise topology for Oracle WebCenter Portal. It contains the following sections:

- [Section 2.1, "Overview of Enterprise Deployment Reference Topology"](#)
- [Section 2.2, "Hardware Requirements for an Enterprise Deployment on Linux"](#)
- [Section 2.3, "Clock Synchronization"](#)
- [Section 2.4, "Identifying the Software Components to Install"](#)
- [Section 2.5, "Road Map for the Reference Topology Installation and Configuration"](#)

2.1 Overview of Enterprise Deployment Reference Topology

This section describes the enterprise topology for WebCenter Portal. Use this section to plan your enterprise deployment topology.

This section covers these topics:

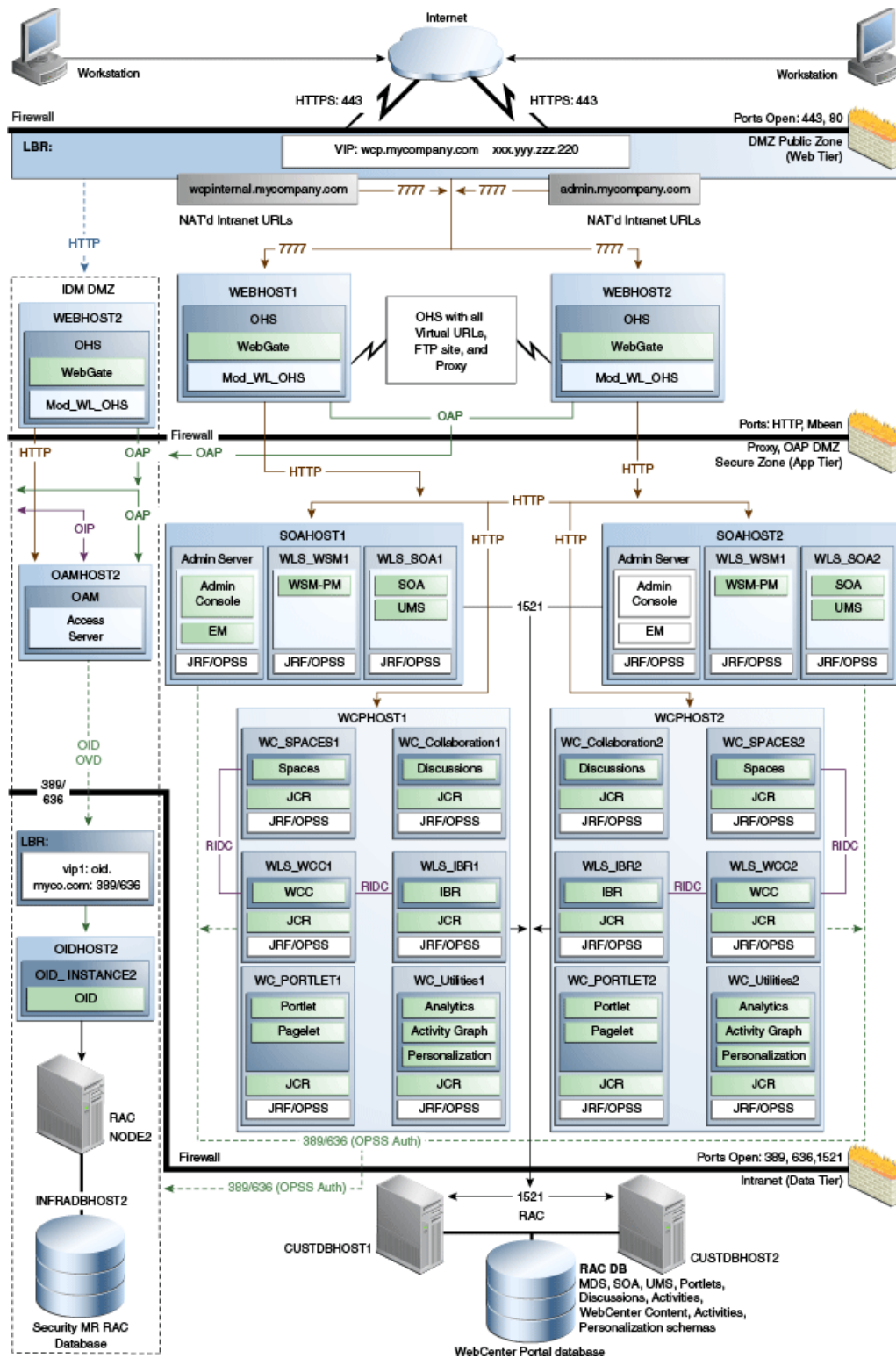
- [Section 2.1.1, "Reference Topology Documented in the Guide"](#)
- [Section 2.1.2, "About Oracle Identity Management Integration"](#)
- [Section 2.1.3, "About the Web Tier Nodes"](#)
- [Section 2.1.4, "About the Application Tier"](#)
- [Section 2.1.5, "About the Data Tier"](#)
- [Section 2.1.6, "About the Unicast Requirement for Communication"](#)

2.1.1 Reference Topology Documented in the Guide

This guide provides configuration instructions for a reference enterprise topology that uses Oracle WebCenter Portal with Oracle Access Manager, as shown in [Figure 2-1](#).

Note: Your actual enterprise deployment topology may require variations on the topology described in this guide.

Figure 2-1 MyWPCCompany Topology with Oracle Access Manager



2.1.2 About Oracle Identity Management Integration

Integration with the Oracle Identity Management system is an important aspect of the enterprise deployment architecture. This integration provides features such as single

sign-on, integration with Oracle Platform Security Services, centralized identity and credential store, and authentication for the WebLogic domain. The Oracle Identity Management (IDM) enterprise deployment is separate from this enterprise deployment and exists in a separate domain by itself. For more information on Oracle Identity Management in an enterprise deployment context, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

The primary interface to the Oracle Identity Management enterprise deployment is the LDAP traffic to the LDAP servers, the OAP (Oracle Access Protocol) to the OAM Access Servers, and the HTTP redirection of authentication requests.

2.1.3 About the Web Tier Nodes

Nodes in the web tier are located in the DMZ public zone.

In this tier, two nodes WEBHOST1 and WEBHOST2 run Oracle HTTP Server configured with WebGate and mod_wl_ohs.

Through mod_wl_ohs, which allows requests to be proxied from Oracle HTTP Server to WebLogic Server, Oracle HTTP Server forwards the requests to WebLogic Server running in the application tier.

WebGate (which is an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on OAMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

The web tier also includes a load balancer router to handle external requests. External requests are sent to the virtual host names configured on the load balancer. The load balancer then forwards the requests to Oracle HTTP Server.

The WebGate module in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager to perform operations such as querying user groups.

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

2.1.3.1 Load Balancer Requirements

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

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration should be possible so that incoming requests on the virtual host name and port are directed to a different port on the backend servers.
- Monitoring of ports on the servers in the pool to determine availability of a service.
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
 - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle HTTP Server in

the web tier, the load balancer needs to be configured with a virtual server and ports for HTTP and HTTPS traffic.

- The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- Sticky routing capability: Ability to maintain sticky connections to components. Examples of this include cookie-based persistence, IP-based persistence, and so on.
- The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the backend real servers using the equivalent non-SSL protocol (for example, HTTPS to HTTP). Typically, this feature is called SSL acceleration and it is required for this Enterprise Deployment.

Note: The load balancer is the entry point for all client requests through the externally facing URL. Although internal URLs are configured as well these are not intended for general use by clients but are for internal use. The WebCenter Portal enterprise deployment topology does not support an 'Inside/Outside' set up.

2.1.4 About the Application Tier

Nodes in the application tier are located in the DMZ secure zone.

In this tier, two nodes SOAHOST1 and SOAHOST2 run the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control, but in an active-passive configuration. You can fail over the Administration Server manually (see [Section 8.6.6, "Manually Failing Over the Administration Server to SOAHOST2"](#)); alternatively you can configure the Oracle WebLogic Server Administration Console with CFC/CRS to fail over automatically on a separate hardware cluster (not shown in this architecture).

Oracle WebCenter Portal components run on WCPHOST1 and WCPHOST2 in an active-active configuration. Typically the managed servers are called WC_Spaces (for the Spaces application), WC_Portlet (for portlet and pagelet producers), WC_Collaboration (for Discussions), and WC_Uutilities (for Analytics, Activity Graph, and Personalization). You can also create custom managed servers to run applications built using WebCenter Portal: Framework.

WCPHOST1 and WCPHOST2 also run Oracle WebCenter Content Server is configured in an active-active manner.

If you are also running SOA components in this topology, SOAHOST1 and SOAHOST2 run on WebLogic Server configured with the WLS_SOA and WLS_WSM managed servers, which run SOA components. These components are configured in an active-active manner.

Oracle Web Services Manager (Oracle WSM) provides a policy framework to manage and secure Web services in the Enterprise Deployment topology. WSM Policy Manager also runs in active-active configuration in two additional WebLogic Servers.

On the firewall protecting the application tier, the HTTP ports, OAP port, and proxy port are open. The OAP port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager. Applications requiring external HTTP access use Oracle HTTP Server as the proxy. (The proxy on the Oracle HTTP Server must be enabled to allow this access.)

2.1.5 About the Data Tier

Nodes in the data tier are located in the most secured network zone (the intranet).

In this tier, an Oracle RAC database runs on the nodes CUSTDBHOST1 and CUSTDBHOST2. The database contains the schemas needed by WebCenter Portal, WebCenter Content, and SOA Suite components. WebCenter Portal, WebCenter Content, and SOA components running in the application tier access this database.

On the firewall protecting the data tier, the database listener port (typically, 1521) is required to be open. The LDAP ports (typically, 389 and 636) are also required to be open for the traffic accessing the LDAP storage in the IDM Enterprise Deployment.

2.1.6 About the Unicast Requirement for Communication

Oracle recommends that the nodes in the MyWCPCompany topology communicate using unicast. Unlike multicast communication, unicast does not require cross-network configuration and it reduces potential network errors that can occur from multicast address conflicts as well.

In unicast messaging mode, the default listening port of the server is used if no channel is configured.

Cluster members communicate to the group leader when they need to send a broadcast message which is usually the heartbeat message. When the cluster members detect the failure of a group leader, the next oldest member becomes the group leader.

The frequency of communication in unicast mode is similar to the frequency of sending messages on multicast port.

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

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

2.2 Hardware Requirements for an Enterprise Deployment on Linux

Before you install and configure your enterprise deployment, review the *Oracle Fusion Middleware System Requirements and Specifications* on the Oracle Technology Network (OTN) to ensure that your environment meets the minimum installation requirements for the products you are installing.

In addition, [Table 2–1](#) lists the typical hardware requirements for the enterprise deployment described in this guide on Linux operating systems.

You must perform the appropriate capacity planning to determine the number of nodes, CPU, and memory requirements for each node depending on the specific system's load, as well as the throughput and response requirements. These will vary for each WebCenter Portal application or custom SOA system being used.

Table 2–1 Typical Hardware Requirements

Server	Disk	Memory	TMP Directory	Swap
Database	nXm n = number of disks, at least 4 (striped as one disk) m = size of the disk (minimum of 30 GB)	6-8 GB	Default	Default
WEBHOST n	10 GB	4 GB	Default	Default
SOAHOST n	10 GB ¹	10 GB	Default	Default
WCPHOST n	10 GB	10 GB	Default	Default

¹ For a shared storage Middleware home configuration, two installations suffice by making a total of 20 GB independently of the number of slots. See also, [Section 4.4, "Configuring Shared Storage"](#).

2.3 Clock Synchronization

The clocks of all servers participating in the cluster must be synchronized to within one second difference to enable proper functioning of jobs, adapters, and Oracle B2B. To accomplish this, use a single network time server and then point each server to that network time server.

The procedure for pointing to the network time server is different on different operating systems. Refer to your operating system documentation for more information.

2.4 Identifying the Software Components to Install

[Table 2–2](#) lists the Oracle software you will need to obtain before starting the procedures in this guide.

For complete information about downloading Oracle Fusion Middleware software, see the *Oracle Fusion Middleware Download, Installation, and Configuration Readme Files* on the Oracle Technology Network (OTN).

See also, *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

Table 2–2 Components and Installation Sources

Component	Distribution Medium
Oracle Database 10g or 11g	Oracle Database 10g distribution (10.2.0.4 or later SE or EE version of the database) using the AL32UTF8 character set. Oracle Database Server 11g distribution (11.1.0.7 or later SE or EE version of the database), using the AL32UTF8 character set.
Repository Creation Utility (RCU)	Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.6) distribution
Oracle WebLogic Server (WLS)	Oracle WebLogic Server (10.3.6) distribution
Oracle HTTP Server (OHS)	Oracle Fusion Middleware WebTier and Utilities 11g (11.1.1.6) distribution
Oracle SOA Suite	Oracle SOA Suite 11g (11.1.1.6) distribution
Oracle WebCenter Portal	Oracle WebCenter Portal 11g (11.1.1.6) distribution
Oracle WebCenter Content	Oracle WebCenter Content 11g (11.1.1.6) distribution
Oracle Access Manager (OAM) WebGate	WebGate 10g (10.1.4.3) for OAM 10g or WebGate 11g (11.1.1.3) for OAM 11g.
Oracle Virtual Directory (OVD)	Oracle Identity and Access Management 11g (11.1.1.5) distribution
Oracle Internet Directory (OID)	Oracle Identity and Access Management 11g (11.1.1.5) distribution

2.5 Road Map for the Reference Topology Installation and Configuration

Before beginning your Oracle WebCenter Portal enterprise deployment, review the flow chart in [Figure 2–2](#). This flow chart illustrates the high-level process for completing the enterprise deployment documented in this guide. [Table 2–3](#) describes the steps in the flow chart and directs you to the appropriate section or chapter for each step.

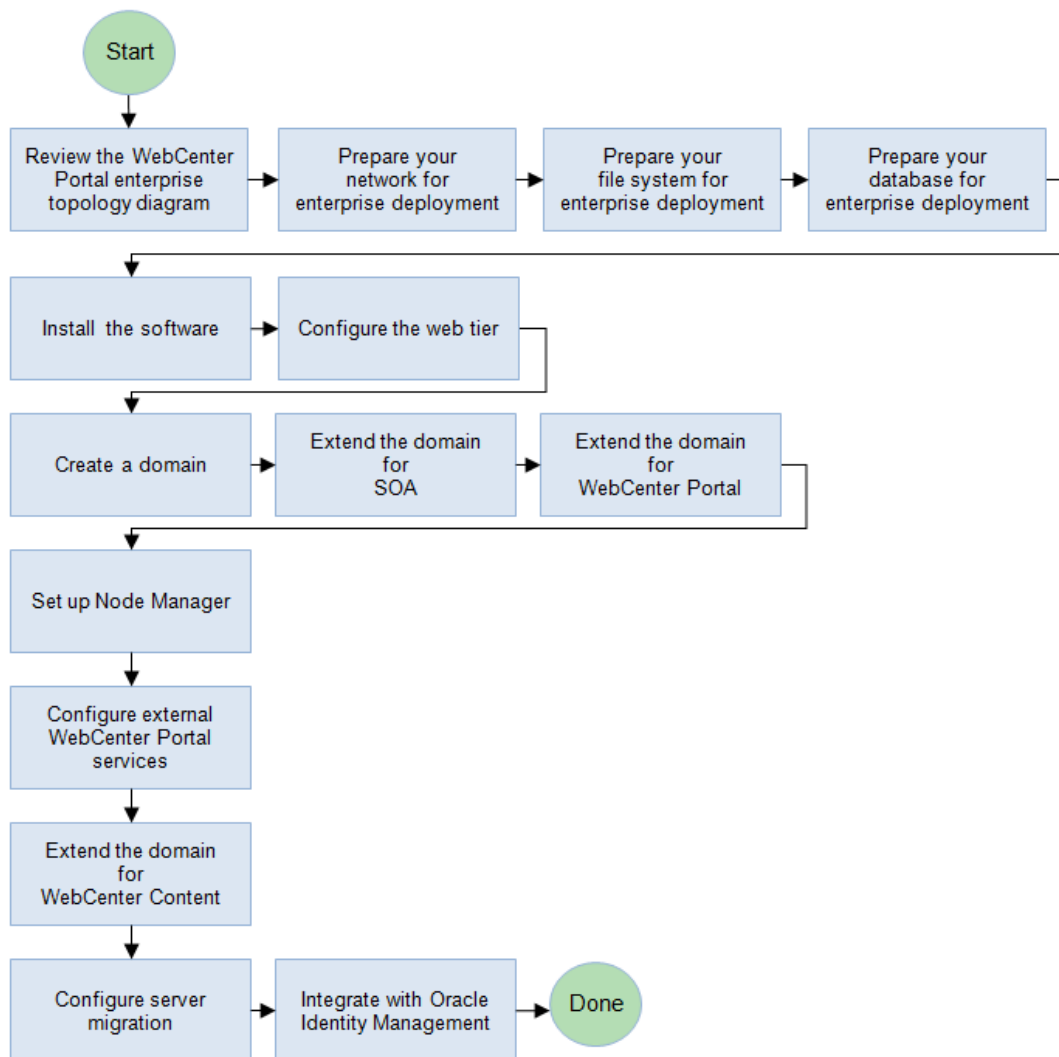
This section covers the following topics:

- [Section 2.5.1, "Flow Chart of the Oracle WebCenter Portal Enterprise Deployment Process"](#)
- [Section 2.5.2, "Steps in the Oracle WebCenter Portal Enterprise Deployment Process"](#)
- [Section 2.5.3, "Understanding the Incremental, Modular Approach to Enterprise Deployment"](#)

2.5.1 Flow Chart of the Oracle WebCenter Portal Enterprise Deployment Process

[Figure 2–2](#) provides a flow chart of the Oracle WebCenter Portal enterprise deployment process. Review this chart to become familiar with the steps that you must follow, based on the existing environment.

Figure 2–2 Flow Chart of the Oracle WebCenter Portal Enterprise Deployment Process



2.5.2 Steps in the Oracle WebCenter Portal Enterprise Deployment Process

Table 2–3 describes each of the steps in the enterprise deployment process flow chart for Oracle WebCenter Portal, shown in Figure 2–2. The table also provides information on where to obtain more information on each step in the process.

Table 2–3 Steps in the Oracle WebCenter Portal Enterprise Deployment Process

Step	Description	More Information
Prepare your network for enterprise deployment	To prepare your network for an enterprise deployment, understand concepts, such as virtual server names and IPs and virtual IPS, and configure your load balancer by defining virtual host names.	Chapter 3, "Preparing the Network for an Enterprise Deployment"
Prepare your file system for enterprise deployment	To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared storage.	Chapter 4, "Preparing the File System for an Enterprise Deployment"
Prepare your database for enterprise deployment	To prepare your database for an enterprise deployment, review database requirements, create database services, load the metadata repository in the Oracle RAC database, configure SOA, WCP, and WCC schemas for transactional recovery privileges, and back up the database.	Chapter 5, "Preparing the Database for an Enterprise Deployment"
Install the software	Install Oracle HTTP Server, Oracle WebLogic Server, Oracle Fusion Middleware, and apply patchsets to Oracle Fusion Middleware components.	Chapter 6, "Installing the Software for an Enterprise Deployment"
Configure the web tier	Configure the Oracle web tier by associating the Oracle web tier with the Oracle WebLogic Domain, Configuring Oracle HTTP Server with the load balancer, and configuring virtual host names.	Chapter 7, "Configuring the Web Tier for an Enterprise Deployment"
Create a domain	Run the Configuration Wizard to create a domain.	Chapter 8, "Creating a Domain for an Enterprise Deployment"
Extend the domain for SOA	Extend the existing WebLogic domain by running the Configuration Wizard to configure Oracle SOA components.	Chapter 9, "Extending the Domain for SOA Components"
Extend the domain for WebCenter Portal	Extend the existing WebLogic domain by running the Configuration Wizard and configure Oracle WebCenter Portal.	Chapter 10, "Extending the Domain for WebCenter Portal Components"
Set up Node Manager	Set up Node manager by enabling host name verification, starting Node Manager, and configuring WebLogic Servers to use custom keystores.	Chapter 11, "Setting Up Node Manager for an Enterprise Deployment"
Configure external WebCenter Portal services	Set up and configure external services for WebCenter Portal applications such as discussions, mail, search, and so on.	Chapter 12, "Configuring External WebCenter Portal Services for an Enterprise Deployment"

Table 2–3 (Cont.) Steps in the Oracle WebCenter Portal Enterprise Deployment Process

Step	Description	More Information
Extend the domain for WebCenter Content	Extend the existing WebLogic domain by running the Configuration Wizard and configure Content Server and Inbound Refinery.	Chapter 13, "Extending the Domain to Include Oracle WebCenter Content"
Configure Server Migration	Configure server migration for the WLS_SOA1 and WLS_SOA2 managed servers. The WLS_SOA1 managed server is configured to restart on SOAHOST2 should a failure occur. The WLS_SOA2 managed server is configured to restart on SOAHOST1 should a failure occur.	Chapter 14, "Configuring Server Migration for an Enterprise Deployment"
Integrate with Identity Management	You can integrate your Oracle SOA enterprise deployment with Oracle Identity Management 10g or 11g.	Chapter 15, "Integrating an Enterprise Deployment with Oracle Identity Management"

2.5.3 Understanding the Incremental, Modular Approach to Enterprise Deployment

By design, this document describes an incremental and modular approach to setting up an enterprise deployment.

The instructions for setting up the storage, database, networking, and web tier infrastructure are similar to the instructions provided in the other Oracle Fusion Middleware Enterprise Deployment Guides. These elements of the topology provide the foundation for the Oracle WebLogic Server domain you later configure to support the enterprise deployment.

When you create the domain, the instructions vary from guide to guide. However, all the Enterprise Deployment Guides provide separate, modular instructions for creating and extending an Oracle WebLogic Server domain, as follows:

1. Install the Oracle Fusion Middleware software on disk and create the necessary binary directories.
2. Run the Oracle Fusion Middleware Configuration Wizard to create the domain and configure only the administration components.

The administration components include the Administration Server, Oracle WebLogic Server Administration Console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Web Services Manager.

3. Run the Configuration Wizard again to extend the domain to include the primary Oracle Fusion Middleware product you want to use.
4. Optionally, run the Configuration Wizard again to extend the domain to include other supporting components and products.

This incremental approach allows you to verify the environment after each pass of the Configuration Wizard. It also simplifies troubleshooting during the setup process.

In addition, this modular approach allows you to consider alternative topologies. Specifically, after you configure the Administration components, the domain you create does not need to contain all the components described in this guide. Instead, you can use the domain extension chapters independently and selectively, to configure individual components that are required for your specific organization.

Preparing the Network for an Enterprise Deployment

This chapter describes the network environment preconfiguration required by the WebCenter Portal enterprise topology. Use this chapter to plan your configuration of virtual server names, load balancers, IPs and Virtual IPs, and firewalls and ports.

This chapter includes the following topics:

- [Section 3.1, "Overview of Preparing the Network for an Enterprise Deployment"](#)
- [Section 3.2, "About Virtual Server Names Used by the Topology"](#)
- [Section 3.3, "Configuring the Load Balancer"](#)
- [Section 3.4, "About IPs and Virtual IPs"](#)
- [Section 3.5, "About Firewalls and Ports"](#)
- [Section 3.6, "About LDAP as Credential and Policy Store"](#)

3.1 Overview of Preparing the Network for an Enterprise Deployment

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

3.2 About Virtual Server Names Used by the Topology

The WebCenter Portal enterprise topology uses the following virtual server names:

- [Section 3.2.1, "wcp.mycompany.com"](#)
- [Section 3.2.2, "admin.mycompany.com"](#)
- [Section 3.2.3, "wcpinternal.mycompany.com"](#)

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

You will define the virtual server names on the load balancer using the procedure in [Section 3.3, "Configuring the Load Balancer."](#)

Note: The only virtual server name which is accessed by clients is the externally facing URL `wcp.mycompany.com`. All other URLs are for internal use only. See also, [Section 2.1.3.1, "Load Balancer Requirements"](#).

3.2.1 `wcp.mycompany.com`

`wcp.mycompany.com` is a virtual server name that acts as the access point for all HTTP traffic to runtime SOA and WebCenter Portal components, such as soa-infra, Workflow, and the Spaces application. Traffic to SSL is configured. Clients access this service using the address `wcp.mycompany.com:443`.

This virtual server is defined on the load balancer.

3.2.2 `admin.mycompany.com`

`admin.mycompany.com` is a virtual server name that acts as the access point for all internal HTTP traffic that is directed to administration services such as WebLogic Administration Server Console and Oracle Enterprise Manager.

The incoming traffic from clients is not SSL-enabled. Clients access this service using the address `admin.mycompany.com:80` and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2.

This virtual server is defined on the load balancer.

3.2.3 `wcpinternal.mycompany.com`

`wcpinternal.mycompany.com` is a virtual server name used for internal invocations of Oracle WebCenter Portal services. This url is not exposed to the internet and is only accessible from the intranet.

The incoming traffic from clients is not SSL-enabled. Clients access this service using the address `wcpinternal.mycompany.com:80` and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2.

This virtual server is defined on the load balancer.

3.3 Configuring the Load Balancer

This enterprise topology uses an external load balancer. Configure the load balancer by defining the virtual server names described in [Section 3.2, "About Virtual Server Names Used by the Topology."](#)

The procedure described below contains high-level steps. The actual steps you will perform vary depending on the type of load balancer you use. For detailed instructions for completing the procedure below consult the documentation for your load balancer.

For more information on load balancers, see [Section 2.1.3, "About the Web Tier Nodes"](#).

Note: For more information on validated load balancers and their configuration, see the following page on Oracle Technology Network at <http://www.oracle.com/technetwork/middleware/ias/tested-lbr-fw-sslaccel-100648.html>.

To configure the load balancer by defining the virtual server names described in [Section 3.2, "About Virtual Server Names Used by the Topology."](#):

1. Create a pool of servers. You will assign this pool to virtual servers.
2. Add the addresses of the Oracle HTTP Server hosts to the pool. For example:
 - `WEBHOST1:7777`
 - `WEBHOST2:7777`
3. Configure a virtual server in the load balancer for `wcp.mycompany.com:443` and define the following rules for this virtual server:
 - For this virtual server, use your system's frontend address as the virtual server address (for example, `wcp.mycompany.com`). The frontend address is the externally facing host name used by your system and that will be exposed in the Internet.
 - Configure this virtual server with port 80 and port 443. Any request that goes to port 80 should be redirected to port 443.
 - Specify **HTTP** as the protocol.
 - Enable address and port translation.
 - Enable reset of connections when services and/or nodes are down.
 - Assign the pool created in step 1 to the virtual server.
 - Create rules to filter out access to `/console` and `/em` on this virtual server.
4. Configure a virtual server in the load balancer for `admin.mycompany.com:80` and define the following rules for this virtual server:
 - For this virtual server, use your internal administration address as the virtual server address (for example, `admin.mycompany.com`). This address is typically not externalized.
 - Specify **HTTP** as the protocol.
 - Enable address and port translation.
 - Enable reset of connections when services and/or nodes are down.
 - Assign the pool created in step 1 to the virtual server.
5. Configure a virtual server in the load balancer for `wcpinternal.mycompany.com:80` and define the following rules for this virtual server:
 - For this virtual server, use the internal address as the virtual server address (for example, `wcpinternal.mycompany.com`). This address is typically not externalized.
 - Specify **HTTP** as the protocol.
 - Enable address and port translation.
 - Enable reset of connections when services and/or nodes are down.
 - Assign the pool created in step 1 to the virtual server.
 - Optionally, create rules to filter out access to `/console` and `/em` on this virtual server.
6. Configure monitors for the Oracle HTTP Server nodes to detect failures in these nodes.

- Set up a monitor to regularly ping the "/" URL context.
Tip: Use `GET /\n\n` instead if the Oracle HTTP Server's document root does not include `index.htm` and Oracle WebLogic Server returns a 404 error for "/".
- For the ping interval, specify a value that does not overload your system. You can try 5 seconds as a starting point.
- For the timeout period, specify a value that can account for the longest time response that you can expect from your WebCenter Portal system, that is, specify a value greater than the longest period of time any of your requests to HTTP servers can take.

After you configure the virtual host in [Section 7.6, "Configuring Virtual Hosts"](#) you should be able to access the virtual host name addresses. If you cannot access them, review this procedure to ensure this procedure was completed correctly.

3.4 About IPs and Virtual IPs

Configure the Administration Server and the managed servers to listen on different virtual IPs and physical IPs as illustrated in [Figure 3–1](#). As shown in this figure, each VIP and IP is attached to the WebLogic server that uses it. VIP1 is failed manually to restart the Administration Server in SOAHOST2. VIP2 and VIP3 fail over from SOAHOST1 to SOAHOST2 and from SOAHOST2 to SOAHOST1 respectively through Oracle WebLogic Server Migration feature. See *Oracle Fusion Middleware High Availability Guide* for information on the WebLogic Server Migration feature.

Physical IPs (non virtual) are fixed to each node:

IP1 is the physical IP of SOAHOST1 and is used by the WLS_WSM1 WebServices Policy Manager server.

IP2 is the physical IP of SOAHOST2 and is used by the WLS_WSM2 WebServices Policy Manager server.

IP3 is the physical IP of WCPHOST1 and is used by all the WebCenter Portal servers (WC_Spaces1, WC_Portlets1, WC_Collaboration1, WC_Uilities1 and ClusterInst1).

IP4 is the physical IP of WCPHOST2 and is used by all the WebCenter Portal servers (WC_Spaces2, WC_Portlets2, WC_Collaboration2, WC_Uilities2 and ClusterInst2).

Figure 3–1 IPs and VIPs Mapped to Administration Server and Managed Servers

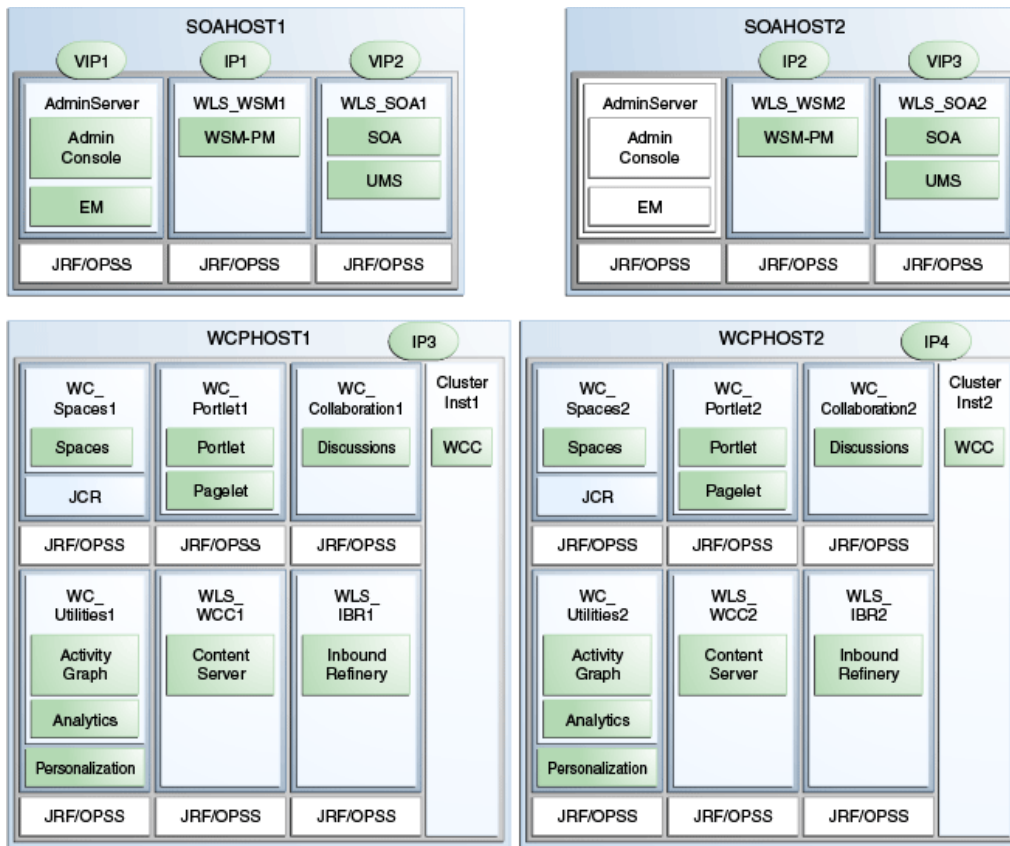


Table 3–1 provides descriptions of the various virtual hosts.

Table 3–1 Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP1	ADMINVHN	ADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running (SOAHOST1 by default).
VIP2	SOAHOST1VHN1	SOAHOST1VHN1 is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA1 process is running (SOAHOST1 by default).
VIP3	SOAHOST2VHN1	SOAHOST2VHN1 is the virtual host name that maps to the listen address for WLS_SOA2 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA2 process is running (SOAHOST2 by default).

3.5 About Firewalls and Ports

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

Most port numbers are assigned during installation.

Table 3–2 lists the ports used in the WebCenter Portal topology, including the ports that you must open on the firewalls in the topology.

Firewall notation:

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

Note: The firewall ports depend on the definition of TCP/IP ports.

Table 3–2 Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for WebCenter Portal.
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for WebCenter Portal.
Browser request	FW1	80	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for SOA.
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for SOA.
Callbacks and Outbound invocations	FW1	80	HTTPS / Load Balancer	Outbound	Timeout depends on all HTML content and the type of process model used for SOA.
Callbacks and Outbound invocations	FW1	443	HTTPS / Load Balancer	Outbound	Timeout depends on all HTML content and the type of process model used for SOA.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 3.3, "Configuring the Load Balancer."
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
OHS management by Administration Server	FW1	OPMN port (6701) and OHS Admin Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period (5-10 seconds).
WSM-PM access	FW1	7010 Range: 7010-7999	HTTP / WLS_ WSM-PM <i>n</i>	Inbound	Set the timeout to 60 seconds.

Table 3–2 (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Communication between WSM Cluster members	n/a	7010	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between Spaces_ Cluster members	n/a	9000	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between Portlet_ Cluster members	n/a	9001	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between Collab_ Cluster members	n/a	9002	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between Utilities_ Cluster members	n/a	9003	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
WebCenter Content access	FW1	16200	HTTP / WLS_ WCC _n	Inbound	Browser-based access. Configurable session timeouts.
Communication between WCC_Cluster members	n/a	16200	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Session replication within a WebLogic Server cluster	n/a	n/a	n/a	n/a	n/a
Administration Console access	FW1	7001	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the admin console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Node Manager	n/a	5556	TCP/IP	n/a	n/a For actual values, see "Firewalls and Ports" in <i>Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management</i> .
Access Server access	FW1	6021	OAP	Inbound	For actual values, see "Firewalls and Ports" in <i>Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management</i> .

Table 3–2 (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Identity Server access	FW1	6022	OAP	Inbound	
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for WebCenter Portal.
Oracle Internet Directory access	FW2	389	LDAP	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
Oracle Internet Directory access	FW2	636	LDAP SSL	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
WebCenter Portal access to WebCenter Content Server	FW2	4444	TCP/IP socket	n/a	Persistent connection. Configurable timeout.
WebCenter Portal access to Inbound Refinery	FW2	5555	TCP/IP socket	n/a	n/a
JOC for OWSM	n/a	9991	TCP/IP	n/a	n/a
Coherence for deployment	n/a	8088 Range: 8000 - 8090		n/a	n/a

3.6 About LDAP as Credential and Policy Store

With Oracle Fusion Middleware, you can use different types of credential and policy stores in a WebLogic domain. Domains can use stores based on XML files or on different types of LDAP providers. When a domain uses an LDAP store, all policy and credential data is kept and maintained in a centralized store. However, when using XML policy stores, the changes made on managed servers are not propagated to the Administration Server unless they use the same domain home.

Note: The domain home is the physical directory from which the server runs, that is, `/aserver` or `/mserver`. Changes made to configuration files in the Administration Server domain directory are propagated out. However, changes made to Managed Server domain directories are overwritten.

An Oracle Fusion Middleware WebCenter Portal Enterprise Deployment Topology uses *different domain homes* for the Administration Server and the managed server as described in the [Chapter 4.3, "About Recommended Locations for the Different Directories"](#). Derived from this, and for integrity and consistency purposes, Oracle requires the use of an LDAP as policy and credential store in context of Oracle Fusion Middleware WebCenter Portal Enterprise Deployment Topology.

To configure the WebCenter Portal Enterprise Deployment Topology with an LDAP as Credential and Policy store, follow the steps in [Section 15.2, "Configuring the Credential Store"](#) and [Section 15.3, "Configuring the Policy Store."](#)

Preparing the File System for an Enterprise Deployment

This chapter describes how to prepare your file system for an Oracle WebCenter Portal enterprise deployment. It provides information about recommended directory structure and locations, and includes a procedure for configuring shared storage.

This chapter includes the following topics:

- [Section 4.1, "Overview of Preparing the File System for Enterprise Deployment"](#)
- [Section 4.2, "Terminology for Directories and Directory Environment Variables"](#)
- [Section 4.3, "About Recommended Locations for the Different Directories"](#)
- [Section 4.4, "Configuring Shared Storage"](#)

4.1 Overview of Preparing the File System for Enterprise Deployment

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

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

4.2 Terminology for Directories and Directory Environment Variables

This section describes the directory environment variables used throughout this guide for configuring the Oracle WebCenter Portal enterprise deployment. The following directory variables are used to describe the directories installed and configured in the guide:

- **ORACLE_BASE:** This environment variable and related directory path refers to the base directory under which Oracle products are installed.
- **MW_HOME:** This environment variable and related directory path refers to the location where Fusion Middleware (FMW) resides.
- **WL_HOME:** This environment variable and related directory path contains installed files necessary to host a WebLogic Server.

- **ORACLE_HOME:** This environment variable and related directory path refers to the location where either Oracle SOA Suite or Oracle WebCenter Portal is installed.
- **ORACLE_COMMON_HOME:** This environment variable and related directory path refers to the Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).
- **DOMAIN Directory:** This directory path refers to the location where the Oracle WebLogic Domain information (configuration artifacts) is stored. Different Oracle WebLogic Servers can use different domain directories even when in the same node as described below.
- **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.

Tip: You can simplify directory navigation by using environment variables as shortcuts to the locations in this section. For example, you could use an environment variable called `$ORACLE_BASE` in Linux to refer to `/u01/app/oracle` (that is, the recommended `ORACLE_BASE` location). In Windows, you would use `%ORACLE_BASE%` and use Windows-specific commands.

4.3 About Recommended Locations for the Different Directories

With Oracle Fusion Middleware 11g you can create multiple SOA or WebCenter Portal servers from one single binary installation. This allows the installation of binaries in a single location on a shared storage and the reuse of this installation by the servers in different nodes. However, for maximum availability, Oracle recommends using redundant binary installations. In the Enterprise Deployment model, two MW HOMEs (each of which has a `WL_HOME` and an `ORACLE_HOME` for each product suite) are installed in a shared storage. Additional servers (when scaling out or up) of the same type can use either one of these two locations without requiring more installations. Ideally, users should use two different volumes (referred to as `VOL1` and `VOL2` below) for redundant binary location, thus isolating as much as possible the failures in each volume. For additional protection, Oracle recommends that these volumes are disk mirrored. If multiple volumes are not available, Oracle recommends using mount points to simulate the same mount location in a different directory in the shared storage. Although this does not guarantee the protection that multiple volumes provide, it does allow protection from user deletions and individual file corruption.

When an `ORACLE_HOME` or a `WL_HOME` is shared by multiple servers in different nodes, it is recommended to maintain the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the `oraInventory` in a node and "attach" an installation in a shared storage to it, use `ORACLE_HOME/oui/bin/attachHome.sh`. To update the Middleware home list to add or remove a `WL_HOME`, edit the `<user_home>/bea/beahomelist` file. This would be required for any nodes installed additionally to the two ones used in this Enterprise Deployment. An example of the `oraInventory` and `beahomelist` updates is provided in the scale-out steps included in this guide.

Oracle recommends also separating the domain directory used by the Administration Server from the domain directory used by managed servers. This allows a symmetric configuration for the domain directories used by managed server, and isolates the failover of the Administration Server. The domain directory for the Administration

Server must reside in a shared storage to allow failover to another node with the same configuration. The managed servers' domain directories can reside in a local or shared storage.

You can use a shared domain directory for all managed servers in different nodes or use one domain directory per node. Sharing domain directories for managed servers facilitates the scale-out procedures. In this case, the deployment should conform to the requirements (if any) of the storage system to facilitate multiple machines mounting the same shared volume. The configuration steps provided in this Enterprise Deployment Topology assume that a local (per node) domain directory is used for each managed server

All procedures that apply to multiple local domains apply to a single shared domain. Hence, this enterprise deployment guide uses a model where one domain directory is used per node. The directory can be local or reside in shared storage.

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

Based on the above assumptions, the following paragraphs describe the directories recommended. Wherever a shared storage location is directly specified, it is implied that shared storage is required for that directory. When using local disk or shared storage is optional the mount specification is qualified with "if using a shared disk." The shared storage locations are examples and can be changed as long as the provided mount points are used. However, Oracle recommends this structure in the shared storage device for consistency and simplicity.

ORACLE_BASE:

/u01/app/oracle

Domain Directory for Administration Server Domain Directory:

ORACLE_BASE/admin/domain_name/aserver/domain_name (The last "domain_name" is added by Configuration Wizard)

- Mount point on machine: *ORACLE_BASE/admin/domain_name/aserver*
- Shared storage location: *ORACLE_BASE/admin/domain_name/aserver*
- Mounted from: Only the node where the Administration Server is running needs to mount this directory. When the Administration Server is relocated (failed over) to a different node, the node then mounts the same shared storage location on the same mount point. The remaining nodes in the topology do not need to mount this location

Domain Directory for Managed Server Domain Directory:

ORACLE_BASE/admin/domain_name/mserver/domain_name

- If you are using a shared disk, the mount point on the machine is *ORACLE_BASE/admin/domain_name/mserver* mounted to *ORACLE_BASE/admin/domain_name/Noden/mserver/* (each node uses a different domain directory for managed servers).

Note: This procedure is really shared storage dependent. The above example is specific to NAS, but other storage types may provide this redundancy with different types of mappings.

Location for JMS file-based stores and Tlogs (SOA only):

ORACLE_BASE/admin/domain_name/soa_cluster_name/jms

ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs

- Mount point: *ORACLE_BASE/admin/domain_name/soa_cluster_name/*
- Shared storage location: *ORACLE_BASE/admin/domain_name/soa_cluster_name/*
- Mounted from: All nodes running SOA must mount this shared storage location so that transaction logs and JMS stores are available when server migration to another node take place.

Location for Application Directory for the Administration Server

ORACLE_BASE/admin/domain_name/aserver/applications

- Mount point: *ORACLE_BASE/admin/domain_name/aserver/*
- Shared storage location: *ORACLE_BASE/admin/domain_name/aserver*
- Mounted from: Only the node where the Administration Server is running must mount this directory. When the Administration Server is relocated (failed over) to a different node, the node then mounts the same shared storage location on the same mount point. The remaining nodes in the topology do not need to mount this location

Location for Application Directory for Managed Server

ORACLE_BASE/admin/domain_name/mserver/applications

Note: This directory is local in the context of a SOA enterprise deployment.

MW_HOME (application tier)

ORACLE_BASE/product/fmw

- Mount point: *ORACLE_BASE/product/fmw*
- Shared storage location: *ORACLE_BASE/product/fmw* (VOL1 and VOL2)

Note: When there is just one volume available in the shared storage, you can provide redundancy using different directories to protect from accidental file deletions and for patching purposes. Two MW_HOMEs would be available; at least one at *ORACLE_BASE/product/fmw1*, and another at *ORACLE_BASE/product/fmw2*. These MW_HOMEs are mounted on the same mount point in all nodes.

- Mounted from: Nodes alternatively mount VOL1 or VOL2 so that at least half of the nodes use one installation, and half use the other.

In a WebCenter Portal enterprise deployment topology, SOAHOST1 and WCPHOST1 mounts VOL1 and SOAHOST2 and WCPHOST2 mounts VOL2. When only one volume is available, nodes mount the two suggested directories in shared storage alternately. For example, SOAHOST1 would use *ORACLE_BASE/product/fmw1* as a shared storage location, and SOAHOST2 would use *ORACLE_BASE/product/fmw2* as a shared storage location)

MW_HOME (web tier):

ORACLE_BASE/product/fmw/web

- Mount point: ORACLE_BASE/product/fmw
- Shared storage location: ORACLE_BASE/product/fmw (VOL1 and VOL2)

Note: Web tier installation is typically performed on local storage to the WEBHOST nodes. When using shared storage, consider the appropriate security restrictions for access to the storage device across tiers.

This enterprise deployment guide assumes that the Oracle web tier will be installed onto local disk. You may install the Oracle Web Tier binaries (and the ORACLE_INSTANCE) onto shared disk. If so, the shared disk MUST be separate from the shared disk used for the application tier.

- Mounted from: For Shared Storage installations, nodes alternatively mount VOL1 or VOL2 so that at least half of the nodes use one installation, and half use the other.

In a WebCenter Portal enterprise deployment topology, WEBHOST1 mounts VOL1 and WEBHOST2 mounts VOL2. When only one volume is available, nodes mount the two suggested directories in shared storage alternately. For example, WEBHOST1 would use *ORACLE_BASE/product/fmw1* as a shared storage location, and WEBHOST2 would use *ORACLE_BASE/product/fmw2* as a shared storage location).

WL_HOME:

MW_HOME/wlserver_10.3

ORACLE_HOME:

- *MW_HOME/wc* (Oracle home for WebCenter Portal)
- *MW_HOME/soa* (Oracle home for SOA Suite)
- *MW_HOME/wcc* (Oracle home for WebCenter Content)

ORACLE_COMMON_HOME:

MW_HOME/oracle_common

ORACLE_INSTANCE (OHS instance):

ORACLE_BASE/admin/instance_name

- If you are using a shared disk, the mount point on the machine is:

ORACLE_BASE/admin/instance_name

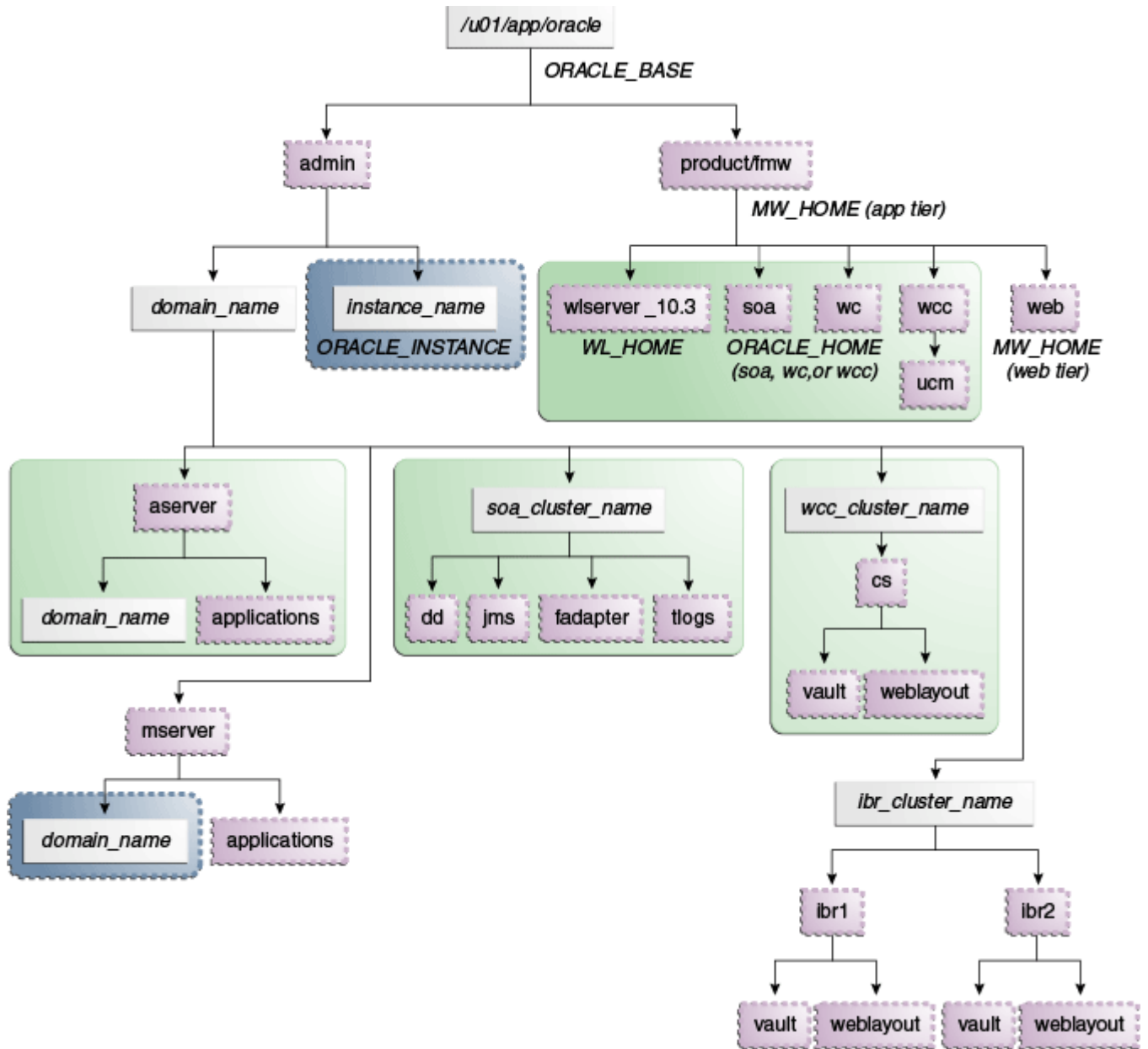
Mounted to:

ORACLE_BASE/admin/instance_name (VOL1)

Note: (VOL1) is optional; you could also use (VOL2).

Figure 4–1 shows this directory structure in a diagram.

Figure 4–1 Directory Structure



The directory structure in Figure 4–1 does not show other required internal directories, such as oracle_common and jrockit.

Table 4–1 explains what the various color-coded elements in the diagram mean.

Table 4–1 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.

Table 4–1 (Cont.) Directory Structure Elements




Element	Explanation
	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 <code>instance_name</code> directory for the web tier can be on a local disk or a shared disk.
	Fixed name.
	Installation-dependent name.

Figure 4–2 shows an example configuration for shared storage with multiple volumes for WebCenter Portal. The example shows SOAHOST1 and SOAHOST2. In addition, managed server directories on WCPHOST1 and WCPHOST2 appear on VOL1 and VOL2 as shown.

Figure 4–2 Example Configuration for Shared Storage

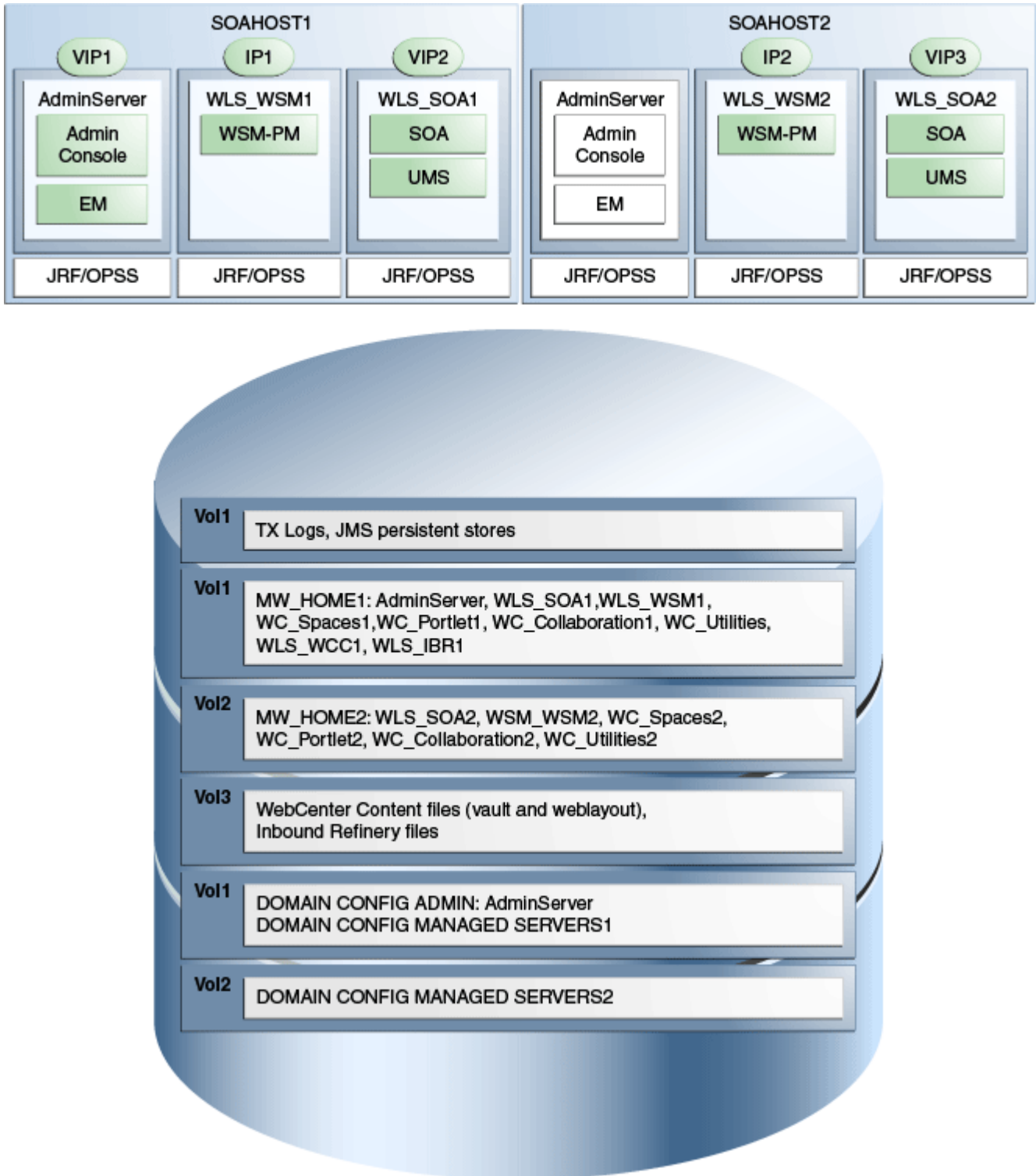


Table 4–2 summarizes the directory structure for the domain. In the table:

- WLS_WCP refers to all the WebCenter Portal managed servers: WC_Spaces, WC_Portlet, WC_Uilities, WC_Collaboration

- **WLS_WCC** refers to the WebCenter Content managed server **WLS_WCC**, and includes **WLS_IBR**.

Table 4–2 Content of Shared Storage

Server	Type of Data	Volume in Shared Storage	Directory	Files
WLS_SOA1	Tx Logs	VOL1	<i>ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs</i>	The transaction directory is common (decided by WebLogic Server), but the files are separate.
WLS_SOA2	Tx Logs	VOL1	<i>ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs</i>	The transaction directory is common (decided by WebLogic Server), but the files are separate.
WLS_SOA1	JMS Stores	VOL1	<i>ORACLE_BASE/admin/domain_name/soa_cluster_name/jms</i>	The transaction directory is common (decided by WebLogic Server), but the files are separate; for example: SOAJMSStore1, UMSJMSStore1, and so on.
WLS_SOA2	JMS Stores	VOL1	<i>ORACLE_BASE/admin/domain_name/soa_cluster_name/jms</i>	The transaction directory is common (decided by WebLogic Server), but the files are separate; for example: SOAJMSStore2, UMSJMSStore2, etc.
WLS_SOA1	WLS Install	VOL1	<i>MW_HOME</i>	Individual in each volume, but both servers see same directory structure.
WLS_SOA2	WLS Install	VOL2	<i>MW_HOME</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP1	WLS Install	VOL1	<i>MW_HOME</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP2	WLS Install	VOL2	<i>MW_HOME</i>	Individual in each volume, but both servers see same directory structure.
WLS_SOA1	SOA Install	VOL1	<i>MW_HOME/soa</i>	Individual in each volume, but both servers see same directory structure.
WLS_SOA2	SOA Install	VOL2	<i>MW_HOME/soa</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP1	WebCenter Portal Install	VOL1	<i>MW_HOME/wc</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP2	WebCenter Portal Install	VOL2	<i>MW_HOME/wc</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCC1	WebCenter Content Install	VOL1	<i>MW_HOME/wcc</i>	Individual in each volume, but both servers see same directory structure.

Table 4–2 (Cont.) Content of Shared Storage

Server	Type of Data	Volume in Shared Storage	Directory	Files
WLS_WCC2	WebCenter Content Install	VOL2	<i>MW_HOME/wcc</i>	Individual in each volume, but both servers see same directory structure.
WLS_SOA1	Domain Config	VOL1	<i>ORACLE_BASE/admin/domain_name/aserver/domain_name</i>	Used by only one Server where the Administration server is running.
WLS_SOA1	Domain Config	VOL1	<i>ORACLE_BASE/admin/domain_name/mserver/domain_name</i>	Individual in each volume, but both servers see same directory structure.
WLS_SOA2	Domain Config	VOL2	<i>ORACLE_BASE/admin/domain_name/mserver/domain_name</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP1	Domain Config	VOL1	<i>ORACLE_BASE/admin/domain_name/mserver/domain_name</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCP2	Domain Config	VOL2	<i>ORACLE_BASE/admin/domain_name/mserver/domain_name</i>	Individual in each volume, but both servers see same directory structure.
WLS_WCC1	Web and Vault Files	VOL3	<i>ORACLE_BASE/admin/domain_name/wcc_cluster_name/vault</i>	Directory for vault files on a separate volume with locking disabled.
WLS_WCC1	Web and Vault Files	VOL3	<i>ORACLE_BASE/admin/domain_name/wcc_cluster_name/weblayout</i>	Directory for weblayout files on a separate volume with locking disabled.
WLS_WCC2	Web and Vault Files	VOL3	<i>ORACLE_BASE/admin/domain_name/wcc_cluster_name/vault</i>	Directory for vault files on a separate volume with locking disabled.
WLS_WCC2	Web and Vault Files	VOL3	<i>ORACLE_BASE/admin/domain_name/wcc_cluster_name/weblayout</i>	Directory for weblayout files on a separate volume with locking disabled.
WLS_IBR1	Inbound Refinery Files	VOL3	<i>ORACLE_BASE/admin/domain_name/ibr_cluster_name/ibrn</i>	Directory for all inbound refinery files on a separate volume with locking disabled.

Note: VOL3 is mounted as an *NFS nolock volume*. For details, see [Section 4.4, "Configuring Shared Storage"](#).

4.4 Configuring Shared Storage

Use the following commands to create and mount shared storage locations so that SOAHOST1, SOAHOST2, WCPHOST1, and WCPHOST2 can see the same location for binary installation in two separate volumes.

Note: The user ID used to create a shared storage file system owns and has read, write, and execute privileges for those files. Other users in the operating system group can read and execute the files, but they do not have write privileges. For more information about installation and configuration privileges, see the "Understanding Installation and Configuration Privileges and Users" section in the *Oracle Fusion Middleware Installation Planning Guide*.

nasfiler is the shared storage filer.

From SOAHOST1 and WCPHOST1:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/product/fmw
ORACLE_BASE/product/fmw -t nfs
```

From SOAHOST2 and WCPHOST2:

```
mount nasfiler:/vol/vol2/ORACLE_BASE/product/fmw
ORACLE_BASE/product/fmw -t nfs
```

If only one volume is available, users can provide redundancy for the binaries by using two different directories in the shared storage and mounting them to the same directory in the SOA Servers:

From SOAHOST1:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/product/fmw1
ORACLE_BASE/product/fmw -t nfs
```

From SOAHOST2:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/product/fmw2
ORACLE_BASE/product/fmw -t nfs
```

The following commands show how to share the SOA TX logs location across different nodes:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/soadomain/soa_cluster/tlogs
ORACLE_BASE/stores/soadomain/soa_cluster/tlogs -t nfs
```

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/soadomain/soa_cluster/tlogs
ORACLE_BASE/stores/soadomain/soa_cluster/tlogs -t nfs
```

From WCPHOST1 and WCPHOST2:

The following commands show how to share WebCenter Content and Inbound Refinery files across different nodes:

```
mount nasfiler:/vol/vol3/ORACLE_BASE/admin/wcdomain/wcc_cluster/vault
-t nfs -o rw,bg,hard,vers=3,nolock
```

```
mount nasfiler:/vol/vol3/ORACLE_BASE/admin/wcdomain/ibr_cluster/
nfs -o rw,bg,hard,vers=3,nolock
```

And likewise for WCPHOST2.

Validating the Shared Storage Configuration

Ensure that you can read and write files to the newly mounted directories by creating a test file in the shared storage location you just configured.

For example:

```
$ cd newly mounted directory
$ touch testfile
```

Verify that the owner and permissions are correct:

```
$ ls -l testfile
```

Then remove the file:

```
$ rm testfile
```

Note: The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from SOAHOST1. The options may differ depending on the specific storage device.

```
mount nasfiler:/vol/vol1/fmw11shared ORACLE_BASE/wls -t nfs -o
rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768, wsize=32768
```

Contact your storage vendor and machine administrator for the correct options for your environment.

Preparing the Database for an Enterprise Deployment

This chapter describes procedures for preparing your database for an Oracle WebCenter Portal enterprise deployment. The procedures include initial setup of the database, loading the metadata repository, and backing up the database.

This chapter includes the following topics:

- [Section 5.1, "Overview of Preparing the Database for an Enterprise Deployment"](#)
- [Section 5.2, "About Database Requirements"](#)
- [Section 5.3, "Creating Database Services"](#)
- [Section 5.4, "Loading the Oracle Fusion Metadata Repository in the Oracle RAC Database"](#)
- [Section 5.5, "Configuring SOA Schemas for Transactional Recovery Privileges"](#)
- [Section 5.6, "Backing Up the Database"](#)

5.1 Overview of Preparing the Database for an Enterprise Deployment

For the WebCenter Portal enterprise topology, the database contains the Oracle Fusion Middleware Repository, which is a collection of schemas used by various Oracle Fusion Middleware components, such as the WebCenter Portal components, and OWSM. This database is separate from the Identity Management database, which is used in Identity Management Enterprise Deployment by components such as Oracle Internet Directory, DIP, and so on.

You must install the Oracle Fusion Middleware Repository before you can configure the Oracle Fusion Middleware components. You install the Oracle Fusion Middleware metadata repository into an existing database using the Repository Creation Utility (RCU), which is available from the RCU DVD or from the location listed in [Table 2-2](#). For the enterprise topology, a Real Application Clusters (Oracle RAC) database is highly recommended.

Later on, when you configure WebCenter Portal components, the configuration wizard will prompt you to enter the information for connecting to the database that contains the metadata repository.

5.2 About Database Requirements

Before loading the metadata repository into your database, check that the database meets the requirements described in these subsections:

- [Section 5.2.1, "Database Host Requirements"](#)
- [Section 5.2.2, "Supported Database Versions"](#)
- [Section 5.2.3, "About Initialization Parameters"](#)

5.2.1 Database Host Requirements

On the hosts CUSTDBHOST1 and CUSTDBHOST2 in the data tier, note the following requirements:

- **Oracle Clusterware**
For 11g Release 1 (11.1) for Linux, refer to the *Oracle Clusterware Installation Guide for Linux*.
- **Oracle Real Application Clusters**
For 11g Release 1 (11.1) for Linux, refer to the *Oracle Real Application Clusters Installation Guide for Linux and UNIX*. For 10g Release 2 (10.2) for Linux, refer to *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide*.
- **Automatic Storage Management (optional)**
ASM gets installed for the node as a whole. It is recommended that you install it in a separate Oracle Home from the Database Oracle Home. This option comes in at runInstaller. In the Select Configuration page, select the **Configure Automatic Storage Management** option to create a separate ASM home.

5.2.2 Supported Database Versions

Oracle WebCenter Portal requires the presence of a supported database and schemas:

To check if your database is certified or to see all certified databases, refer to the "Oracle Fusion Middleware 11g Release 1 (11.1.1.x)" product area on the *Oracle Fusion Middleware Supported System Configurations* page:

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

To check the release of your database, you can query the PRODUCT_COMPONENT_VERSION view as follows:

```
SQL> SELECT VERSION FROM SYS.PRODUCT_COMPONENT_VERSION WHERE  
PRODUCT LIKE 'Oracle%';
```

Note: Oracle WebCenter Portal requires the database be used to store its metadata (either 10g or 11g) supports the **AL32UTF8** character set. Check the database documentation for information on choosing a character set for the database.

5.2.3 About Initialization Parameters

Ensure that the following initialization parameter is set to the required minimum value. It is checked by Repository Creation Utility.

Table 5–1 Required Initialization Parameters

Configuration	Parameter	Required Value	Parameter Class
SOA	PROCESSES	300 or greater	Static
WebCenter Portal	PROCESSES	300 or greater	Static
SOA and WebCenter Portal	PROCESSES	600 or greater	Static
SOA, WebCenter Portal, and WebCenter Content	PROCESSES	700 or greater	Static

To check the value of the initialization parameter using SQL*Plus, you can use the SHOW PARAMETER command.

As the SYS user, issue the SHOW PARAMETER command as follows:

```
SQL> SHOW PARAMETER processes
```

Set the initialization parameter using the following command:

```
SQL> ALTER SYSTEM SET processes=300 SCOPE=SPFILE;
```

Restart the database.

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

5.3 Creating 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*.

You can also use SQL*Plus to configure this using the following instructions:

1. Use the CREATE_SERVICE subprogram to create the wcpedg.mycompany.com database service. Log on to SQL*Plus as the sysdba user and run the following command:

```
SQL> EXECUTE DBMS_SERVICE.CREATE_SERVICE
(SERVICE_NAME => 'wcpedg.mycompany.com',
NETWORK_NAME => 'wcpedg.mycompany.com',
);
```

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

```
prompt> srvctl add service -d wcdb -s wcpedg.mycompany.com -r wcdb1,wcdb2
```

3. Start the service using srvctl:

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

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

5.4 Loading the Oracle Fusion Metadata Repository in the Oracle RAC Database

The Repository Creation Utility (RCU) is available from the RCU distribution. The RCU used to seed the database must match the patch set level of the Oracle WebCenter Portal installation. This means that if you install Oracle WebCenter Portal 11gR1 (11.1.1.6) in this enterprise deployment, you must use RCU 11gR1 (11.1.1.6).

To load the Oracle Fusion Middleware Repository into a database:

1. Open the Repository Creation Utility (RCU) distribution.
2. Start RCU from the *bin* directory in the RCU home directory:

```
cd RCU_Home/bin
./rcu
```
3. In the Welcome screen, click **Next**.
4. In the Create Repository screen, select **Create** to load component schemas into a database. Click **Next**.
5. In the Database Connection Details screen, enter the correct information for your database:
 - **Database Type:** select **Oracle Database**.
 - **Host Name:** Enter the name of the node that is running the database. For the Oracle RAC database, specify the VIP name or one of the node names as the host name: CUSTDBHOST1-VIP.
 - **Port:** Enter the port number for the database: 1521.
 - **Service Name:** Enter the service name of the database: wcpedg.mycompany.com
 - **Username:** SYS
 - **Password:** Enter the password for the SYS user.
 - **Role:** SYSDBAClick **Next**.
6. If you get this warning message: The database you are connecting is with non-UTF8 charset, if you are going to use this database for multilingual support, you may have data loss. If you are not using for multilingual support you can continue, otherwise we strongly recommend using UTF-8 database.
Click **Ignore** or **Stop**.
7. In the Select Components screen, do the following:
 - a. Select **Create a New Prefix**, and enter a prefix to use for the database schemas. For example, wcpedg. Prefixes are used to create logical groupings of multiple repositories in a database. For more information, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
 - b. Note the name of the schema because you will need the information later on.

- c. Select the following:
- AS Common Schemas:
 - **Metadata Services**
 - SOA Infrastructure:
 - **SOA and BPM Infrastructure**
 - **User Messaging Service**
 - WebCenter Portal (select all schemas):
 - **Spaces and Services**
 - **Portlet Producers**
 - **Activity Graph and Analytics**
 - **Discussions**

Note: This will auto-select **Metadata Services** as well.

- WebCenter Content:
 - **Oracle WebCenter Content Server - Complete**

Click **Next**.

8. In the Schema Passwords screen, select **Use main schema passwords for auxiliary schemas** and click **Next**. In the subsequent screen refresh, enter the schema passwords for all components.

Tip: Note the name of the schema because the upcoming steps require this information.

9. In the Map Tablespaces screen, choose the tablespaces for the selected components, and click **Next**.

A confirmation dialog is displayed stating that any tablespace that does not already exist in the selected schema will be created. Click **OK** to acknowledge this message.

10. In the Summary screen, click **Create**.

11. In the Completion Summary screen, click **Close**.

12. Verify that the required schemas are created by connecting to the database with the new user added:

```
ORACLE_HOME/bin/sqlplus
```

For example, log in as the **WCPEDG_WEBCENTER** user and enter the password. A simple verification can be performed by querying the schema version registry:

```
-bash-3.00$ $ORACLE_HOME/bin/sqlplus WCPEDG_WEBCENTER/password as SYSDBA
SQL> SELECT version, status FROM schema_version_registry where owner =
'WCPEDG_WEBCENTER';
```

```
VERSION STATUS
```

```
-----
11.1.1.6.0 VALID
```

About Oracle WSM policies and the OWSM MDS schemas

If Oracle WSM is part of your WebCenter Portal enterprise deployment, Oracle recommends using the identity management database to store the Oracle WSM policies. Use the IM database connection information for the OWSM MDS schemas instead of the information used for the rest of SOA/WebCenter Portal schemas. To create the required schemas in the database, repeat the steps above (run RCU again) using the IM database information, but select only **AS Common Schemas: Metadata Services** in the Select Components screen (step 7). See [Section 15, "Integrating an Enterprise Deployment with Oracle Identity Management"](#) for information on using the identity management database to store the Oracle WSM policies.

5.5 Configuring SOA Schemas for Transactional Recovery Privileges

You need the appropriate database privileges to allow the Oracle WebLogic Server transaction manager to query for transaction state information and issue the appropriate commands, such as commit and rollback, during recovery of in-flight transactions after a WebLogic Server container crash.

These privileges should be granted to the owner of the `soainfra` schema, as determined by the RCU operations.

To configure the SOA schemas for transactional recovery privileges:

1. Log on to sqlplus as a user with sysdba privileges. For example:

```
sqlplus "/ as sysdba"
```

2. Enter the following commands:

```
SQL> Grant select on sys.dba_pending_transactions to wcpedg_soainfra_soainfra;
```

```
Grant succeeded.
```

```
SQL> Grant force any transaction to wcpedg_soainfra_soainfra;
```

```
Grant succeeded.
```

```
SQL>
```

5.6 Backing Up the Database

After you have loaded the metadata repository into your database, make a backup before installing the software for your enterprise deployment.

Backing up the database is for the explicit purpose of quick recovery from any issue that may occur in the further steps. You can choose to use your backup strategy for the database for this purpose or simply make a backup using operating system tools or RMAN for this purpose. Oracle recommends to use Oracle Recovery Manager for the database, particularly if the database was created using Oracle ASM. If possible, you can also perform a cold backup using operating system tools such as tar.

Installing the Software for an Enterprise Deployment

This chapter describes the software installations required for the enterprise deployment reference topology for Oracle WebCenter Portal. You install Oracle HTTP Server and then Oracle Fusion Middleware.

This chapter contains the following sections:

- [Section 6.1, "Overview of the Software Installation Process"](#)
- [Section 6.2, "Installing Oracle HTTP Server"](#)
- [Section 6.3, "Installing Oracle Fusion Middleware"](#)

6.1 Overview of the Software Installation Process

The enterprise deployment software installation is divided into two parts. The first part covers the required web tier installations, while the second part addresses the required Fusion Middleware (FMW) components. Later chapters describe the required configuration steps to create the reference topology for Oracle WebCenter Portal.

Obtaining the Software

For information about where to obtain the software, See "Obtain the Oracle Fusion Middleware Software" in the *Oracle Fusion Middleware Installation Planning Guide* for information on where to obtain the software.

Select one of the download locations and download "Oracle WebCenter Portal." The .zip archive file is saved to your system.

After you download the archive file, extract the archive file into a directory of your choice on the machine where you are performing the installation.

Software to Install

[Table 6–1](#) shows what software should be installed on each host or be accessible from each host.

Table 6–1 Software To Be Installed On Each Host or Accessible From Each Host

Hosts	Oracle HTTP Server	Oracle WebLogic Server	Oracle SOA Suite	Oracle WebCenter Portal	Oracle WebCenter Content
WEBHOST1	X				
WEBHOST2	X				

Table 6–1 (Cont.) Software To Be Installed On Each Host or Accessible From Each Host

Hosts	Oracle HTTP Server	Oracle WebLogic Server	Oracle SOA Suite	Oracle WebCenter Portal	Oracle WebCenter Content
SOAHOST1		X	X	X	X
SOAHOST2		X	X	X	X
WCPHOST1		X	X	X	X
WCPHOST2		X	X	X	X

6.2 Installing Oracle HTTP Server

This section covers these topics:

- [Section 6.2.1, "Prerequisites to Installing Oracle HTTP Server"](#)
- [Section 6.2.2, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2"](#)
- [Section 6.2.3, "Backing Up the Oracle Fusion Middleware Installation"](#)

6.2.1 Prerequisites to Installing Oracle HTTP Server

Prior to installing Oracle HTTP Server (OHS), check that your machines meet the following requirements:

- Ensure that the system, patch, kernel, and other requirements are met as specified in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.
- Because Oracle HTTP Server is installed on port 7777 by default, you must make sure that port 7777 is not used by any service on the nodes. To check if this port is in use, run the following command before installing Oracle HTTP Server:

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

You must free port 7777 if it is in use.

- On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct. Specifically, 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.
- Before starting the installation, make sure that the following environment variables are not set:
 - LD_ASSUME_KERNEL
 - ORACLE_INSTANCE

6.2.2 Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2

As described in [Chapter 4, "Preparing the File System for an Enterprise Deployment,"](#) you install Oracle Fusion Middleware in at least two storage locations for redundancy.

To install Oracle HTTP Server on WEBHOST1 and WEBHOST2:

1. Start the installer for Oracle HTTP Server from the installation media:


```
./runInstaller
```
2. In the Specify Inventory Directory screen, do the following:

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

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

Click **OK**.

3. In the **Welcome** screen, click **Next**.
4. In the **Install Software Updates** screen, choose **Skip Software Updates** and click **Next**.
5. In the **Select Installation Type** screen, select **Install - Do Not Configure**, and click **Next**.
6. In the **Prerequisite Checks** screen, verify that all checks complete successfully, and click **Next**.
7. In the **Specify Installation Location** screen, specify the following:
 - **Fusion Middleware Home Location** (installation location): `ORACLE_BASE/product/fmw`
 - **Oracle Home Location Directory**: `web`

Click **Next**.

8. In the **Specify Security Updates** screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.
9. In the **Installation Summary** screen, review the selections to ensure they are correct. If they are not, click **Back** to modify selections on previous screens. When you are ready, click **Install**.

On UNIX systems, if prompted to run the `oracleRoot.sh` script, make sure you run it as the root user.

The Oracle HTTP Server software is installed.

10. In the **Installation Completed** screen, click **Finish** to exit.
11. Validate the installation by verifying that the following directories appear in the `ORACLE_HOME` directory after installing Oracle HTTP Server:
 - `oracle_common`
 - `web`

6.2.3 Backing Up the Oracle Fusion Middleware Installation

The Fusion Middleware Home should be backed up now (make sure no server is running at this point):

```
WEBHOST1> tar -cvpf fmwhomeback.tar ORACLE_BASE/product/fmw HOME/oraInventory
```

6.3 Installing Oracle Fusion Middleware

This section describes how to install the required Oracle Fusion Middleware software for the enterprise deployment reference topology for Oracle WebCenter Portal. The software components to be installed consist of the Oracle WebLogic Server Home (`WL_HOME`) and Oracle Home (`ORACLE_HOME`). As described in [Chapter 4](#),

"[Preparing the File System for an Enterprise Deployment](#)," you install Oracle Fusion Middleware in at least two storage locations for redundancy.

Note: Before starting the setup process, read the *Oracle Fusion Middleware Release Notes* for additional installation and deployment information.

This section covers these topics:

- [Section 6.3.1, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#)
- [Section 6.3.2, "Installing Oracle Fusion Middleware Components"](#)
- [Section 6.3.3, "Backing Up the Fusion Middleware Installation"](#)

6.3.1 Installing Oracle WebLogic Server and Creating the Fusion Middleware Home

Install Oracle WebLogic Server on SOAHOST1, SOAHOST2, WCPHOST1, and WCPHOST2.

Note: If you are installing WebLogic Server on a 64-bit platform using a 64-bit JDK, follow the steps in section "Installing WebLogic Server on 64-Bit Platforms Using a 64-Bit JDK" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* instead of the steps in this section.

To install Oracle WebLogic Server:

1. Start the installer for Oracle WebLogic Server from the installation media:

```
$ ./wls1036_linux32.bin
```

2. In the Welcome screen, click **Next**.
3. In the Choose Middleware Home Directory screen, do the following:
 - Select **Create a new Middleware Home**.
 - For Middleware Home Directory, enter `ORACLE_BASE/product/fmw`

Note: See [Section 4, "Preparing the File System for an Enterprise Deployment"](#) for more information.

ORACLE_BASE is the base directory under which Oracle products are installed. The recommended value is `/u01/app/oracle`. See [Section 4.3, "About Recommended Locations for the Different Directories"](#) for more information.

Click **Next**.

4. In the **Register for Security Updates** screen, enter your contact information so that you can be notified of security updates, and click **Next**.
5. In the **Choose Install Type** screen, select **Custom**, and click **Next**.
6. In the **Choose Products and Components** screen, click **Next**.

7. In the **JDK Selection** screen, select *only* **Oracle JRockit 1.6.0_<version> SDK**, and click **Next**.
8. In the **Choose Product Installation Directories** screen, accept the directories **ORACLE_BASE/product/fmw/wlserver_10.3** and **ORACLE_BASE/product/fmw/coherence_3.7**, and click **Next**.
9. In the **Installation Summary** screen, click **Next**.
The Oracle WebLogic Server software is installed.
10. In the **Installation Complete** screen, clear the **Run Quickstart** check box and click **Done**.

6.3.2 Installing Oracle Fusion Middleware Components

This section covers these topics:

- [Section 6.3.2.1, "Installing Oracle SOA Suite"](#)
- [Section 6.3.2.2, "Installing Oracle WebCenter Portal"](#)
- [Section 6.3.2.3, "Installing Oracle WebCenter Content"](#)

6.3.2.1 Installing Oracle SOA Suite

To install Oracle SOA Suite on SOAHOST1, SOAHOST2, WCPHOST1, and WCPHOST2:

Note: Since the installation is performed on a shared storage, the MW_HOME is accessible and used by Oracle WebCenter Portal in WCPHOST1 and WCPHOST2.

1. On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct. Specifically, 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.
2. Start the installer for Oracle SOA Suite from the installation media:

```
./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-jdk1.6.0_version`. For more information, see [Section 6.3.1, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#).

3. In the Specify Inventory Directory screen, do the following:
 - a. Enter **HOME/oraInventory**, where *HOME* is the home directory of the user performing the installation (this is the recommended location).
 - b. Enter the Operating System Group name for the user performing the installation.
 - c. Click **OK**.

Follow the instructions on screen to execute `/createCentralInventory.sh` as root. Click **OK**.

Note: The Specify Inventory Directory screen appears only on a UNIX operating system, for the first installation by Oracle Universal Installer. The installer will use the inventory directory to keep track of all Oracle products installed on the machine.

4. In the Welcome screen, click **Next**.
5. In the Install Software Updates screen, choose Skip Software Updates and click **Next**.
6. In the Prerequisite Checks screen, verify that all checks complete successfully, and click **OK**.
7. In the Specify Installation Location screen, provide the installation location for Oracle SOA Suite. Select the previously installed Oracle Middleware Home from the drop-down list. For the Oracle Home directory, enter the SOA Suite directory name (**soa**).

Figure 6–1 Specify Installation Location Screen in Installer Wizard



Click **Next** when you are done.

8. In the Application Server screen, select **WebLogic Server** and click **Next**.
9. In the Installation Summary screen, click **Install**.
The Oracle Fusion Middleware SOA Suite software is installed.
10. In the Installation Complete screen, click **Finish**.
11. Validate the installation by verifying that the following files and directories appear in the ORACLE_HOME directory after installing both Oracle WebLogic Server and Oracle SOA Suite:
 - coherence_X.X

- jrockit-jdkY.Y
- modules
- oracle_common
- registry.xml
- utils
- domain-registry.xml
- logs
- ocm.rsp
- registry.dat
- soa
- wlsserver_10.3

6.3.2.2 Installing Oracle WebCenter Portal

To install Oracle WebCenter Portal on SOAHOST1, SOAHOST2, WCPHOST1, and WCPHOST2:

1. Start the installer for Oracle WebCenter Portal:

```
./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-jdk1.6.0_version*. For more information, see [Section 6.3.1, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#).

2. In the Specify Inventory Directory screen, do the following:
 - a. Enter *HOME/oraInventory*, where *HOME* is the home directory of the user performing the installation (this is the recommended location).
 - b. Enter the Operating System Group name for the user performing the installation.
 - c. Click **OK**.

Note: The Specify Inventory Directory screen appears only on a UNIX operating system, for the first installation by Oracle Universal Installer. The installer will use the inventory directory to keep track of all Oracle products installed on the machine.

3. In the Welcome screen, click **Next**.
4. In the Install Software Updates screen, choose **Skip Software Updates** and click **Next**.
5. In the Prerequisite Checks screen, verify that all checks complete successfully, and click **OK**.
6. In the Specify Installation Location screen, provide the installation location for Oracle WebCenter Portal. Select the previously installed Oracle Middleware Home from the drop-down list. For the Oracle Home directory, enter the WebCenter Portal directory name (**wc**).

Click **Next**.

7. In the Application Server screen, select **WebLogic Server** and click **Next**.
8. In the Installation Summary screen, click **Install**.
The Oracle WebCenter Portal software is installed.
9. In the Installation Complete screen, click **Finish**.
10. Validate the installation by verifying that the following directories and files appear in the ORACLE_HOME directory after installing both Oracle WebLogic Server, Oracle SOA Suite, and Oracle WebCenter Portal:
 - coherence_version
 - jrockit-jdkversion
 - modules
 - oracle_common
 - registry.xml
 - utils
 - domain-registry.xml
 - logs
 - ocm.rsp
 - registry.dat
 - soa
 - wc
 - wlsserver_10.3

6.3.2.3 Installing Oracle WebCenter Content

To install Oracle WebCenter Content on SOAHOST1, SOAHOST2, WCPHOST1, and WCPHOST2:

1. Start the installer for Oracle WebCenter Content:

```
./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-jdk1.6.0_version`. For more information, see [Section 6.3.1, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home."](#)

2. In the Welcome screen, click **Next**.
3. In the Install Software Updates screen, choose Skip Software Updates and click **Next**.
4. In the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.
5. In the Specify Installation Location screen, provide the installation location for Oracle WebCenter Content. Select the previously installed Oracle Middleware Home from the drop-down list. For the Oracle Home directory, enter directory name (**wcc**).

Click **Next** when you are done.

6. In the Application Server screen, make sure **WebLogic Server** is selected (which is the default), and click **Next**.
7. In the Installation Summary screen, click **Install**.
The Oracle WebCenter Content software is installed.
8. In the Installation Complete screen, click **Finish**.
9. Validate the installation by verifying that the following directories and files appear in the *ORACLE_HOME* directory after installing Oracle WebLogic Server, Oracle Fusion Middleware for SOA, Oracle WebCenter Portal, and Oracle WebCenter Content:
 - *coherence_version*
 - *jrocket-jdkversion*
 - *modules*
 - *oracle_common*
 - *registry.xml*
 - *utils*
 - *domain-registry.xml*
 - *logs*
 - *ocm.rsp*
 - *registry.dat*
 - *soa*
 - *wc*
 - *wlserver_10.3*
 - *wcc*

6.3.3 Backing Up the Fusion Middleware Installation

The Fusion Middleware Home should be backed up now from SOAHOST1 (make sure that you stop the servers first):

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

This creates a backup of the installation files for both Oracle WebLogic Server and Oracle Fusion Middleware components.

Configuring the Web Tier for an Enterprise Deployment

This chapter describes how to configure the Oracle Web Tier to support the Oracle Fusion Middleware WebCenter Portal implementation.

This chapter contains the following sections:

- [Section 7.1, "Overview of Configuring the Web Tier"](#)
- [Section 7.2, "Running the Configuration Wizard to Configure Oracle HTTP Server"](#)
- [Section 7.3, "Validating the Oracle HTTP Server Configuration"](#)
- [Section 7.4, "Associating the Oracle Web Tier with the Oracle WebLogic Domain"](#)
- [Section 7.5, "Configuring the Load Balancer to Route HTTP Requests"](#)
- [Section 7.6, "Configuring Virtual Hosts"](#)

7.1 Overview of Configuring the Web Tier

Before configuring the Oracle Web Tier software, you must install it on WEBHOST1 and WEBHOST2, as described in [Section 6.2, "Installing Oracle HTTP Server"](#). Run the Configuration Wizard to define the instance home, the instance name, and the Oracle HTTP Server component name.

This chapter also describes how to associate the Oracle Web Tier with the WebLogic Server domain. Once the web tier is associated with the WebLogic Server, you can monitor it using the Oracle Fusion Middleware Console.

You then configure the load balancer to route all HTTP requests to WEBHOST1 and WEBHOST2.

The last section describes how to define the directives of the `<VirtualHost>` section of the `httpd.conf` file on both OHS servers. You created these virtual host names when you configured the load balancer in [Section 3.3, "Configuring the Load Balancer"](#).

7.2 Running the Configuration Wizard to Configure Oracle HTTP Server

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

To configure the Oracle web tier:

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

```
WEBHOST1> cd ORACLE_COMMON_HOME/common/bin
```

2. Start the Configuration Wizard:

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

3. In the Welcome screen, click **Next**.
4. In the Configure Components screen, select **Oracle HTTP Server** and unselect **Associate Selected Components with WebLogic Domain**. Make sure that Oracle Web Cache is *not* selected.

Click **Next**.

5. In the Specify Component Details screen, specify the following values:

- Instance Home Location: /u01/app/oracle/admin/web*n*
- AS Instance Name: web*n*
- OHS Component Name: ohs*n*

(where *n* is a sequential number for your installation; for example, 1 for WEBHOST1, 2 for WEBHOST2, and so on.)

Note: Oracle HTTP Server instance names on WEBHOST1 and WEBHOST2 must be different.

Click **Next**.

6. In high-availability implementations, it is not mandatory for all of the ports used by the various components to be synchronized across hosts, however it makes the enterprise deployment much simpler. Oracle allows automatic port configuration to be bypassed by specifying ports to be used in a file.

In the Configure Ports screen, select a file name and then click **View/Edit**. The file will look like this:

```
[OHS]
#Listen port for OHS component
OHS Port = 7777

[OPMN]
#Process Manager Local port no
OPMN Local Port = 1880
```

You can find a sample staticports.ini file on installation disk 1 in the stage/Response directory.

Click **Next**.

7. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.
8. In the Installation Summary screen, review the selections to ensure they are correct. If they are not, click **Back** to modify selections on previous screens. When you are ready, click **Configure**.
9. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, click **Next**, and the Installation Complete screen appears.
10. In the Installation Completed screen, click **Finish** to exit.

7.3 Validating the Oracle HTTP Server Configuration

Once the installation is completed, check that it is possible to access the Oracle HTTP Server home page using the following URL:

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

7.4 Associating the Oracle Web Tier with the Oracle WebLogic Domain

Once an Oracle WebLogic domain has been created, the Oracle web tier can be linked to the domain. The advantages of doing this are that the Oracle web tier can be managed and monitored using the Oracle Fusion Middleware console.

To associate the Oracle web tier with the WebLogic domain, execute the following commands on both WEBHOST1 and WEBHOST2:

```
WEBHOSTn> cd ORACLE_BASE/admin/instance_name/bin
WEBHOSTn> ./opmnctl registerinstance -adminHost ADMINVHN -adminPort 7001
-adminUsername weblogic
```

7.5 Configuring the Load Balancer to Route HTTP Requests

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server (WEBHOST1, WEBHOST2). You do not need to enable sticky sessions (insert cookie) on the load balancer when Oracle HTTP Server is front-ending Oracle WebLogic Server. You need sticky sessions 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.

The instructions for this configuration will vary depending on which load balancer you use. See your load balancer documentation for specific instructions.

7.6 Configuring Virtual Hosts

To configure the virtual hosts complete the following three tasks:

- Define the directives of the <VirtualHost> section of the `httpd.conf` file on both OHS servers
- Restart both OHS servers
- Access the virtual host URLs to validate the configuration.

7.6.1 Editing the `httpd.conf` File

Define the directives of the <VirtualHost> section of the `httpd.conf` file on both OHS servers. This file is located in the `ORACLE_BASE/admin/instance_name/config/OHS/ohs1` (or `ohs2`) directory. Add the following entries to the file:

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

NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName admin.mycompany.com:80
```

```
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>

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

7.6.2 Restarting Both OHS Servers

Restart both OHS servers after modifying the httpd.conf files:

```
WEBHOST> cd ORACLE_BASE/admin/<instance_name>/bin
WEBHOST> opmnctl stopall
WEBHOST> opmnctl startall
```

7.6.3 Validating the Configuration

Access the following URLs to ensure that your load balancer and Oracle HTTP Server are configured properly:

- <https://wcp.mycompany.com/index.html>
- <http://admin.mycompany.com/index.html>
- <http://wcpinternal.mycompany.com/index.html>

If you cannot access these URLs, check to ensure that you completed the procedure in [Section 3.3, "Configuring the Load Balancer"](#) correctly.

Creating a Domain for an Enterprise Deployment

This chapter describes how to create a domain using the Configuration Wizard, Oracle WebLogic Server Administration Console, Oracle Enterprise Manager, and Oracle WSM Policy Manager. You can extend the domain to add WebCenter Portal components.

Note: Before starting the setup process, read the *Oracle Fusion Middleware Release Notes* for additional installation and deployment information.

This chapter contains the following sections:

- [Section 8.1, "Overview of Creating a Domain"](#)
- [Section 8.2, "Enabling VIP1 in SOAHOST1"](#)
- [Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain"](#)
- [Section 8.4, "Post-Configuration and Verification Tasks"](#)
- [Section 8.5, "Propagating the Domain Configuration to SOAHOST2"](#)
- [Section 8.6, "Configuring Oracle HTTP Server for the WebLogic Domain"](#)
- [Section 8.7, "Backing Up the WebLogic Domain Configuration"](#)

8.1 Overview of Creating a Domain

[Table 8–1](#) lists the steps for creating a WebLogic domain, including post-configuration tasks.

Table 8–1 Steps for Creating a WebLogic Domain

Step	Description	More Information
Enabling VIP1 in SOAHOST1	Enable a VIP1 for the SOAHOST1 hostname.	Section 8.2, "Enabling VIP1 in SOAHOST1"
Create a WebLogic Domain	Run the Configuration Wizard to create WebLogic domain.	Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain"
Post-Configuration and Verification Tasks	Follow the instructions for post-configuration and validation tasks.	Section 8.4, "Post-Configuration and Verification Tasks"
Propagate the Domain Configuration to SOAHOST2	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory.	Section 8.5, "Propagating the Domain Configuration to SOAHOST2"
Configure the Oracle HTTP Server with the WebLogic domain	Configure the Oracle HTTP Server with the WebLogic domain and validate the configuration.	Section 8.6, "Configuring Oracle HTTP Server for the WebLogic Domain"
Back Up the Domain	Back up the newly configured WebLogic domain.	Section 8.7, "Backing Up the WebLogic Domain Configuration"

Once this domain is created and configured you can extend the domain to include Oracle WebCenter Portal components, Oracle SOA Suite, Oracle WebCenter Content, and so on, described in the next chapters.

8.2 Enabling VIP1 in SOAHOST1

Please note that this step is required for failover of the Administration Server, regardless of whether or not SOA is installed.

You are associating the Administration Server with a virtual hostname (ADMINVHN). This Virtual Host Name must be mapped to the appropriate VIP (VIP1) either by a DNS Server or by a custom `/etc/hosts` entry. Check that ADMINVHN is available according to your name resolution system, (DNS server, `/etc/hosts`), in the required nodes in your SOA topology. The VIP (VIP1) that is associated to this Virtual Host Name (ADMINVHN) must be enabled in SOAHOST1.

To enable the virtual IP on Linux:

1. Run the `ifconfig` command as root:

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

For example:

```
/sbin/ifconfig ethX:Y 100.200.140.206 netmask 255.255.255.0
```

2. Enable your network to register the new location of the virtual IP, for example:

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

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

```
/bin/ping 100.200.140.206
```


In this example 'ethX' is the ethernet interface (eth0 or eth1) and Y is the index (0, 1, 2).

8.3 Running the Configuration Wizard on SOAHOST1 to Create a Domain

Run the Configuration Wizard from the ORACLE_COMMON_HOME directory to create a domain containing the Administration Server and Oracle Web Services Manager. Later, you will extend the domain to contain WebCenter Portal, SOA, and WebCenter Content components.

To create a domain:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, all instances should be running, so that the validation check later in the procedure is more reliable.

2. On SOAHOST1, change directory to the location of the Configuration Wizard:

```
cd ORACLE_COMMON_HOME/common/bin
```

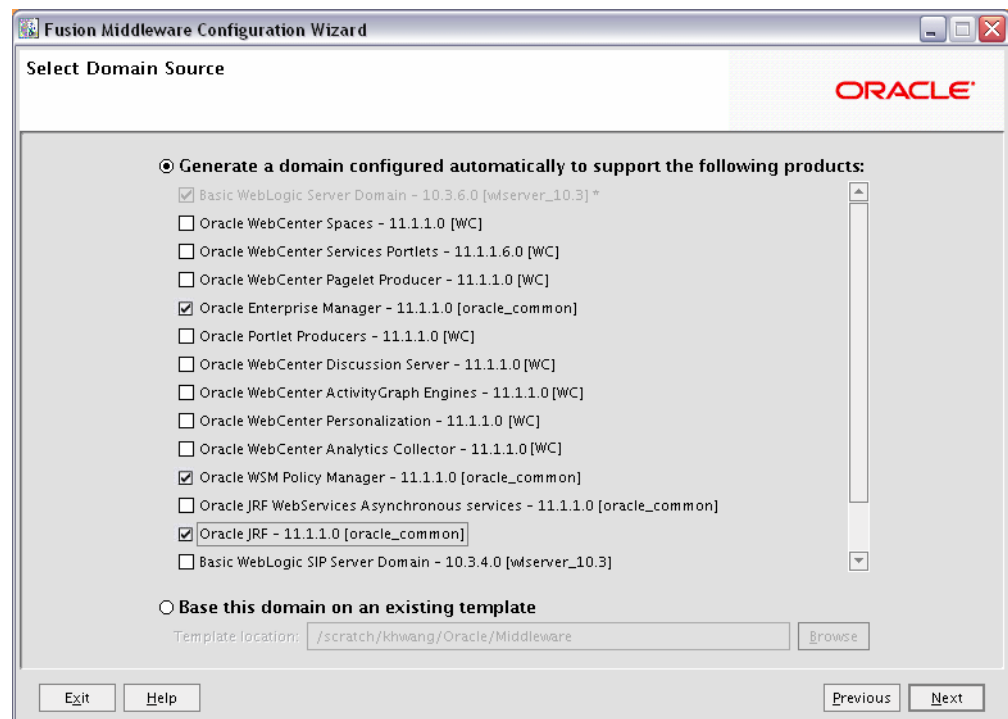
3. Start the Oracle Fusion Middleware Configuration Wizard:

```
./config.sh
```

4. In the Welcome screen, select **Create a New WebLogic Domain**, and click **Next**.

5. The Select Domain Source screen appears (Figure 8–1).

Figure 8–1 Select Domain Source Screen



In 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 - 10.3.6.0 [wlserver_10.3]** (this should be selected automatically)
- **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**
- **Oracle WSM Policy Manager 11.1.1.0 [oracle_common]**
- **Oracle JRF - 11.1.1.0 [oracle_common]** (this should be selected automatically)

If you accidentally deselect some of the targets, make sure that the following selections are made in this screen:

- Oracle Enterprise Manager
- Oracle WSM Policy Manager
- Oracle JRF

Click **Next**.

Note: If multiple Oracle Homes are installed (for example a WebCenter Portal Home and a SOA Home), available products will show up for both homes. In this step, select only products from the WebCenter Portal home (wc). This is indicated by brackets at the end of the product name; for example, "Oracle JRF - 11.1.1.0 [wc]."

6. In the Specify Domain Name and Location screen, enter the domain name (wcpedg_domain).

Make sure that the domain directory matches the directory and shared storage mount point recommended in [Chapter 3, "Preparing the Network for an Enterprise Deployment"](#).

For the domain directory, enter:

ORACLE_BASE/admin/domain_name/aserver

For the application directory, enter (this directory should be in shared storage):

ORACLE_BASE/admin/domain_name/aserver/applications

7. Click **Next**.
8. In the Configure Administrator Username and Password screen, enter the username and password to be used for the domain's administrator.

Click **Next**.

9. In 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_<version>**.

Click **Next**.

10. In the Configure JDBC Components Schema screen, do the following:

- a. Select the OWSM MDS schema.
- b. Select **Configure selected component schemas as RAC multi data source schemas in the next panel**.
- c. Click **Next**.

11. The Configure RAC Multi Data Sources Component Schema screen is displayed (Figure 8–2).

Figure 8–2 Configure RAC Multi Data Source Component Schema Screen

Note: Change only the input fields below that you wish to modify and values will be applied to all selected rows.

Driver: *Oracle's Driver (Thin) for RAC Service-Instance c[...]

Service Name: wcedg.mycompany.com

Username: wcedg_mds

Password: *****

Host Name	Instance Name	Port
custdbhost1-vip.mycom	wcedgdb1	1521
custdbhost2-vip.mycom	wcedgdb2	1521

Add Delete

Multi Data Source Schema	Service Name	Schema Owner	Schema Password
<input checked="" type="checkbox"/> OWSM MDS Schema	wcedg.mycompany.com	wcedg_mds	*****

Exit Help Previous Next

In this screen, do the following:

- a. Enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.
 - **Driver:** Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, 11.**
 - **Service Name:** Enter the service name of the database, for example, wcpedg.mycompany.com.
 - **Username:** Enter the complete user name (including the prefix) for the schemas.
 - **Password:** Enter the password to use to access the schemas.
 - b. Enter the host name, instance name, and port.
 - c. Click **Add**.
 - d. Repeat this for each Oracle RAC instance.
 - e. Click **Next**.
12. In the Test JDBC Data Sources screen, the connections should be tested automatically. The **Status** column displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen and correct your entries.
- Click **Next** when all the connections are successful.

13. In the Select Advanced Configuration screen, select the following:

- **Administration Server**
- **Managed Servers, Clusters and Machines**
- **Deployment and Services**

Click **Next**.

14. In the Configure the Administration Server screen, enter the following values:

- Name: **AdminServer**
- Listen Address: enter ADMINVHN.
- Listen Port: **7001**
- SSL listen port: **N/A**
- SSL enabled: **unchecked**

Click **Next**.

15. In the Configure Managed Servers screen, click **Add** to add the following managed servers:

Table 8–2 Managed Servers

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_WSM1	SOAHOST1	7010	n/a	No
WLS_WSM2	SOAHOST2	7010	n/a	No

Click **Next**.

16. In the Configure Clusters screen, Click **Add** to add the following clusters:

Table 8–3 Clusters

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
WSM-PM_Cluster	unicast	n/a	n/a	Leave it empty.

Click **Next**.

17. In the Assign Servers to Clusters screen, assign servers to clusters as follows:

- **WSM-PM_Cluster:**
 - WLS_WSM1
 - WLS_WSM2

Click **Next**.

18. In the Configure Machines screen, do the following:

- Click the **Unix Machine** tab and then click **Add** to add the following machines:

Note: "Name" can be any unique string. "Node Manager Listen Address" must be a resolvable host name.

Table 8–4 Machines

Name	Node Manager Listen Address
SOAHOST1	SOAHOST1
SOAHOST2	SOAHOST2
ADMINHOST	localhost

Leave all other fields to their default values.

Click **Next**.

19. In the **Assign Servers to Machines** screen, assign servers to machines as follows:

- **SOAHOST1:** WLS_WSM1
- **SOAHOST2:** WLS_WSM2
- **ADMINHOST:** AdminServer

Click **Next**.

20. In the **Target Deployments to Clusters or Servers** screen, make sure that the **wsm-pm** application and the **oracle.wsm.seedpolicies** library is targeted to the **WSM-PM_Cluster** only. Make sure that all other deployments are targeted to the **AdminServer**. Click **Next**.

21. In the **Target Services to Clusters or Servers** screen, select the following:

- On the left, select **WSM-PM_Cluster**. On the right, select **JDBC System Resource** (this automatically selects all the wsm datasources (mds-owsm)).
- On the left, select **Admin Server**. On the right, select **JDBC System Resource** (this automatically selects all the wsm datasources (mds-owsm)).

All JDBC system resources should be targeted to both the Admin Server and WSM-PM_Cluster.

- Make sure that all the remaining services are targeted to the **Admin Server**.
- Click **Next**.

22. In the **Configuration Summary** screen, click **Create**.

23. In the **Create Domain** screen, click **Done**.

8.4 Post-Configuration and Verification Tasks

After configuring the domain with the Configuration Wizard, follow these instructions for post-configuration and verification.

The section includes the following topics:

- [Section 8.4.1, "Creating boot.properties for the Administration Server on SOAHOST1"](#)
- [Section 8.4.2, "Starting Node Manager on SOAHOST1"](#)
- [Section 8.4.3, "Starting the Administration Server on SOAHOST1"](#)
- [Section 8.4.4, "Validating the Administration Server Configuration"](#)
- [Section 8.4.5, "Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server"](#)

- [Section 8.4.6, "Applying the Java Required Files \(JRF\) Template to the WSM-PM_Cluster"](#)
- [Section 8.4.7, "Disabling Host Name Verification for the Administration Server and the WLS_WSM1 Managed Server"](#)
- [Section 8.4.8, "Starting and Validating the WLS_WSM1 Managed Server"](#)

8.4.1 Creating `boot.properties` for the Administration Server on SOAHOST1

Create a `boot.properties` file for the Administration Server on SOAHOST1. This is a required step that enables you to start the Administration Server using Node Manager.

To create a `boot.properties` file for the Administration Server:

1. Create the following directory structure:

```
mkdir -p ORACLE_BASE/admin/domain_name/aserver/domain_
name/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 following lines in the file:

```
username=Admin_Username
password=Password
```

Note: When you start the Administration Server, the username and password entries in the file get encrypted. You start the Administration Server in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

For security reasons, you want to minimize the time the entries in the file are left unencrypted: after you edit the file, you should start the server as soon as possible so that the entries get encrypted.

3. Save the file and close the editor.

8.4.2 Starting Node Manager on SOAHOST1

If you are starting Node Manager for the first time, set the `StartScriptEnabled` property to 'true', and then start Node Manager using `startNodeManager.sh`.

To start Node Manager on SOAHOST1:

1. Before starting Node Manager for the first time, run the `setNMProps.sh` script, which is located in the `ORACLE_COMMON_HOME/common/bin` directory, to set the `StartScriptEnabled` property to 'true':

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

Note: You must set the `StartScriptEnabled` property to avoid class loading failures and other problems; you only need to do this once.

2. Start Node Manager:

```
cd WL_HOME/server/bin
```

```
export JAVA_OPTIONS="-DDomainRegistrationEnabled=true"
./startNodeManager.sh
```

Note: It is important that you set `-DDomainRegistrationEnabled=true` whenever a Node Manager is started that must manage the AdminServer. This is due to the fact that the AdminServer domain home does not exist in the Node Manager Domains file and you must use dynamic registration of the domain. Oracle does not recommend using this parameter except in the case specified here.

If there is no AdminServer on this machine and this machine is not an AdminServer failover node, you should start the Node Manager as:

```
./startNodeManager.sh
```

8.4.3 Starting the Administration Server on SOAHOST1

The Administration Server is started and stopped using Node Manager. However, the first start of the Administration Server with Node Manager, requires changing the defaulted username and password that are set for Node Manager by the Configuration Wizard. Therefore, use the start script for the Administration Server for the first start.

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

To start the Administration Server using Node Manager:

1. Start the Administration Server using the start script in the domain directory on SOAHOST1:

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

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

- a. In a browser, go to the following URL;

```
http://ADMINVHN:7001/console
```

- b. Log in as the administrator.

- c. Click **Lock & Edit**.

- d. Click **domain_name**, **Security, General**, and then expand the **Advanced** options 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 Administration Server process by using **CTRL-C** in the shell where it was started, or by process identification and kill in the operating system.

4. Start WLST and connect to Node Manager with **nmconnect** and the credentials set in the previous steps and start the Administration Server using **nmstart**.

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

Once you are in the WLST shell:

```
wls:/offline>nmConnect("Admin_User", "Admin_Password",  
"SOAHOST1", "5556", "domain_name", "/ORACLE_BASE/admin/domain_name/asever/domain_  
name")  
  
wls:/nm/domain_name nmStart("AdminServer")
```

Note: This username and password are used only to authenticate connections between Node Manager and clients. They are independent of the server admin ID and password and are stored in the `nm_password.properties` file located in the following directory:

```
ORACLE_BASE/admin/domain_name/asever/domain_  
name/config/nodemanager
```

8.4.4 Validating the Administration Server Configuration

To ensure that the Administration Server for the domain you have created is properly configured, validate the configuration by logging into the Oracle WebLogic Server Administration Console and verifying the managed servers and the cluster are listed, and log into Oracle Enterprise Manager.

To verify that the Administration Server is properly configured:

1. In a browser, go to the following URL:

```
http://ADMINVHN:7001/console
```

2. Log in as the administrator.
3. Verify that the **WLS_WSM1** and **WLS_WSM2** managed servers are listed.
4. Verify that **WSM-PM_Cluster** is listed.
5. Check that you can access Oracle Enterprise Manager at the following URL:

```
http://ADMINVHN:7001/em
```

6. Log in to Enterprise Manager Console with the username and password you specified in [Section 8.4.1, "Creating boot.properties for the Administration Server on SOAHOST1."](#)

8.4.5 Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server

Use the `pack` and `unpack` commands to separate the domain directory used by the Administration Server from the domain directory used by the managed server in SOAHOST1 as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment."](#)

Before running the `unpack` script, be sure the `ORACLE_BASE/admin/domain_name/mserver` directory exists as explained in [Chapter 4.3, "About Recommended Locations for the Different Directories."](#)

To create a separate domain directory:

1. Run the `pack` command on SOAHOST1 to create a template pack as follows:

```
SOAHOST1> cd ORACLE_COMMON_HOME/common/bin
```



```
./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=wdomaintemplate.jar -template_name=wdomaintemplate
```

2. Run the unpack command on SOAHOST1 to unpack the template in the managed server domain directory as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=wdomaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

Note: You must have write permissions on the `/ORACLE_BASE/admin/domain_name` directory before running the unpack command. For example, the directory:

```
/ORACLE_BASE/admin/wcpedg_domain/
```

8.4.6 Applying the Java Required Files (JRF) Template to the WSM-PM_Cluster

After the domain is created with the Configuration Wizard, you must target a number of resources not included in the WebLogic server installation to the WSM-PM_Cluster.

To target these resources:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control with the username and password you specified in [Section 8.4.1, "Creating boot.properties for the Administration Server on SOAHOST1."](#)
2. On the navigation tree on the left, expand **Farm_domain_name, WebLogic Domain**, and then **domain_name**, and select **WSM-PM_Cluster**.
3. Click **Apply JRF Template** on the right.
4. Wait for the confirmation message to appear on the screen.

This message should confirm that the JRF Template has been successfully applied to the WSM-PM_Cluster cluster.

8.4.7 Disabling Host Name Verification for the Administration Server and the WLS_WSM1 Managed 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 11, "Setting Up Node Manager for an Enterprise Deployment"](#)). If you have not configured the server certificates, you receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the Enterprise Deployment topology configuration is complete as described in [Chapter 11, "Setting Up Node Manager for an Enterprise Deployment."](#)

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock & 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) appear.
6. Click the **SSL** tab.
7. Click **Advanced**.
8. Set Hostname Verification to **None**.
9. Click **Save**.
10. Repeat steps 4 to 8 for the WLS_WSM1 server.
11. Save and activate the changes.
12. Restart the Administration Server for the changes to take effect:
 - a. In the Summary of Servers screen, select the **Control** tab.
 - b. Select **AdminServer(admin)** in the table and then click **Shutdown**.
 - c. Start the Administration Server again using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

8.4.8 Starting and Validating the WLS_WSM1 Managed Server

After configuring the managed server, start it and check to confirm that it is running properly. You can start the managed server and check its status by using the Oracle WebLogic Server Administration Console.

To start the WLS_WSM1 managed server and check that it is configured correctly:

1. Start the WLS_WSM1 managed server using the Oracle WebLogic Server Administration Console as follows:
 - a. Expand the **Environment** node in the Domain Structure window.
 - b. Choose **Servers**. The Summary of Servers page appears.
 - c. Click the **Control** tab.
 - d. Select **WLS_WSM1** and then click **Start**.
2. Verify that the server status is reported as **Running** in the Admin 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.
3. Access the following URL:
`http://SOAHOST1:7010/wsm-pm`
4. Click **Validate Policy Manager**.

If the configuration is correct, a list of policies and assertion templates available in the data store appear. If the configuration is not correct, no policies or assertion templates appear.

8.5 Propagating the Domain Configuration to SOAHOST2

After completing the configuration of SOAHOST1, propagate the configuration to SOAHOST2 using the unpack utility, and then validate the propagated configuration.

This section includes the following topics:

- [Section 8.5.1, "Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility"](#)
- [Section 8.5.2, "Disabling Host Name Verification for the WLS_WSM2 Managed Server"](#)
- [Section 8.5.3, "Starting Node Manager on SOAHOST2"](#)
- [Section 8.5.4, "Starting and Validating the WLS_WSM2 Managed Server"](#)
- [Section 8.5.5, "Configuring the Java Object Cache for Oracle WSM"](#)

8.5.1 Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility

Propagate the domain configuration using the unpack utility. Before running the unpack script, be sure the following directory exists as explained in [Section 4.3, "About Recommended Locations for the Different Directories"](#).

```
ORACLE_BASE/admin/domain_name/mserver
```

To propagate the domain configuration:

1. Run the following command on SOAHOST1 to copy the template file created previously.

```
cd ORACLE_COMMON_HOME/common/bin
scp wdomaintemplate.jar oracle@SOAHOST2:/ORACLE_COMMON_HOME/common/bin
```

2. Run the unpack command from the ORACLE_COMMON_HOME/common/bin directory, not from the WL_HOME/common/bin directory on SOAHOST2 to unpack the propagated template.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=wdomaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_
name/mserver/applications
```

8.5.2 Disabling Host Name Verification for the WLS_WSM2 Managed 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 11, "Setting Up Node Manager for an Enterprise Deployment"](#)). If you have not configured the server certificates, you will receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the Enterprise Deployment topology configuration is complete as described in [Chapter 11, "Setting Up Node Manager for an Enterprise Deployment."](#)

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page appears.
5. Select **WLS_WSM2** in the Names column of the table. The Settings page for AdminServer(admin) appear.

6. Click the **SSL** tab.
7. Click **Advanced**.
8. Set Hostname Verification to **None**.
9. Save and activate the changes.

8.5.3 Starting Node Manager on SOAHOST2

Once you have propagated the domain configuration and disabled host name verification, start Node Manager using the `StartNodeManager.sh` script.

To start Node Manager on SOAHOST2:

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

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```

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

2. Start Node Manager:

```
cd WL_HOME/server/bin
./startNodeManager.sh
```

8.5.4 Starting and Validating the WLS_WSM2 Managed Server

Use the Administration Console to start and validate the WLS_WSM2 managed server.

To start the WLS_WSM2 managed server and check that it is configured correctly:

1. Start the WLS_WSM2 managed server using the Administration Console.
2. Verify that the server status is reported as **Running** in the Admin 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

3. Access the following URL:

```
http://SOAHOST2:7010/wsm-pm
```

4. Click validate policy manager.

8.5.5 Configuring the Java Object Cache for Oracle WSM

The Java Object Cache (JOC) should be configured among all the servers running Oracle WSM. This local cache is provided to increase the performance of Oracle WSM.

The Java Object Cache can be configured using the `configure-joc.py` script in the following directory:

```
MW_HOME/oracle_common/bin/
```

This is a Python script which can be used to configure JOC in the managed servers. The script runs in WLST online mode and expects the Administration Server to be running.

When configuring JOC ports for Oracle products, Oracle recommends using ports in the 9988 to 9998 range.

Note: After configuring the Java Object Cache using the `wlst` commands or `configure-joc.py` script, all affected managed servers should be restarted for the configurations to take effect.

To configure the Java Object Cache for Oracle WSM:

1. Connect to the Administration Server using the command-line Oracle WebLogic Scripting Tool (WLST), for example:

```
MW_HOME/wc/common/bin/wlst.sh
$ connect()
```

Enter the Oracle WebLogic Administration user name and password when prompted.

2. After connecting to the Administration Server using `wlst`, start the script using the `execfile` command, for example:

```
wls:/mydomain/serverConfig>execfile("MW_HOME/oracle_
common/bin/configure-joc.py")
```

3. Configure JOC for all the managed servers for a given cluster.

Enter 'y' when the script prompts whether you want to specify a cluster name, and also specify the cluster name and discover port, when prompted. This discovers all the managed servers for the given cluster and configure the JOC. The discover port is common for the entire JOC configuration across the cluster. For example:

```
Do you want to specify a cluster name (y/n) <y>
Enter Cluster Name : WSM-PM_Cluster
Enter Discover Port : 9991
```

Here is a walkthrough for using `configure-joc.py` for HA environments:

```
execfile("MW_HOME/oracle_common/bin/configure-joc.py")
.
Enter Hostnames (eg host1,host2) : SOAHOST1,SOAHOST2
.
Do you want to specify a cluster name (y/n) <y>y
.
Enter Cluster Name : WSM-PM_Cluster
.
Enter Discover Port : 9991
.
Enter Distribute Mode (true|false) <true> : true
.
Do you want to exclude any server(s) from JOC configuration (y/n) <n> n
```

The script can also be used to perform the following JOC configurations:

- Configure JOC for all specified managed servers.

Enter 'n' when the script prompts whether you want to specify a cluster name, and also specify the managed server and discover port, when prompted. For example:

```
Do you want to specify a cluster name (y/n) <y>n
Enter Managed Server and Discover Port (eg WLS_WSM1:9998, WLS_WSM1:9998) : WLS_
WSM1:9991,WLS_WSM2:9991
```

- Exclude JOC configuration for some managed servers.

The script allows you to specify the list of managed servers for which the JOC configuration "DistributeMode" will be set to 'false'. Enter 'y' when the script prompts whether you want to exclude any servers from JOC configuration, and enter the managed server names to be excluded, when prompted. For example:

```
Do you want to exclude any server(s) from JOC configuration (y/n) <n>y
Exclude Managed Server List (eg Server1,Server2) : WLS_WSM1,WLS_WSM3
```

- Disable the distribution mode for all managed servers.

The script allows you to disable the distribution to all the managed servers for a specified cluster. Specify 'false' when the script prompts for the distribution mode. By default, the distribution mode is set to 'true'.

Verify JOC configuration using the CacheWatcher utility. See *Oracle Fusion Middleware High Availability Guide*.

You can configure the Java Object Cache (JOC) using the **HA Power Tools** tab in the Oracle WebLogic Administration Console as described in the *Oracle Fusion Middleware High Availability Guide*.

8.6 Configuring Oracle HTTP Server for the WebLogic Domain

This section describes tasks for configuring Oracle HTTP Server for the WebLogic Domain, and for verifying the configuration.

This section includes the following topics:

- [Section 8.6.1, "Configuring Oracle HTTP Server for the Administration Server and the WLS_WSMn Managed Servers"](#)
- [Section 8.6.2, "Turning on the WebLogic Plug-In Enabled Flag"](#)
- [Section 8.6.3, "Registering Oracle HTTP Server With WebLogic Server"](#)
- [Section 8.6.4, "Setting the Frontend URL for the Administration Console and Setting Redirection Preferences"](#)
- [Section 8.6.5, "Validating Access Through Oracle HTTP Server"](#)
- [Section 8.6.6, "Manually Failing Over the Administration Server to SOAHOST2"](#)
- [Section 8.6.7, "Validating Access to SOAHOST2 Through Oracle HTTP Server"](#)
- [Section 8.6.8, "Failing the Administration Server Back to SOAHOST1"](#)

8.6.1 Configuring Oracle HTTP Server for the Administration Server and the WLS_WSMn Managed Servers

To enable Oracle HTTP Server to route to the Administration Server and the WSM-PM_Cluster, which contain the WLS_WSMn managed servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster.

The servers specified in the `WebLogicCluster` parameter are only important at startup time for the plug-in. The list needs to provide at least one running cluster member for the plug-in to discover other members of the cluster. Note that the listed cluster member must be running when Oracle HTTP Server is started. Oracle

WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Some example scenarios:

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

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

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

To set the WebLogicCluster parameter:

1. On WEBHOST1 and WEBHOST2, add lines to the `mod_wl_ohs.conf` file located in the following directory:

```
ORACLE_BASE/admin/instance_name/config/OHS/component_name/
```

Add the following lines:

```
# The admin URLs should only be accessible via the admin virtual host
```

```
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
```

```
    WeblogicPort 7001
```

```
</Location>
```

```
<Location /consolehelp>
```

```
    SetHandler weblogic-handler
```

```
    WebLogicHost ADMINVHN
```

```
    WeblogicPort 7001
```

```
</Location>
```

```
<Location /em>
```

```
    SetHandler weblogic-handler
```

```
    WebLogicHost ADMINVHN
```

```
    WeblogicPort 7001
```

```
</Location>
```

```
</VirtualHost>
```

```
# Virtual host entry for external https URL configured at the Load Balancer
```

```
<VirtualHost *:7777>
```

```
    ServerName https://wcp.mycompany.com:443
```

```

ServerAdmin you@your.address
RewriteEngine On
RewriteOptions inherit

# WSM-PM
<Location /wsm-pm>
  SetHandler weblogic-handler
  WebLogicCluster SOAHOST1:7010,SOAHOST2:7010
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

</VirtualHost>

# Virtual host entry for internal http URL

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

</VirtualHost>

```

Note: Values such as 7777, admin.mycompany.com:80, and you@your.address 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.

```

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

```

```

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

```

8.6.2 Turning on the WebLogic Plug-In Enabled Flag

For security purposes, and since the load balancer terminates SSL request (Oracle HTTP Server routes the requests as non-SSL to WebLogic Server), once you configure SSL for the load balancer, turn on the WebLogic plug-in enabled flag for the domain.

To turn on the WebLogic plug-in enabled flag:

- Log on to the Administration Console.
- Click on the domain name in the navigation tree on the left.
- Click on the **Web Applications** tab.
- Click **Lock & Edit**.
- Select the **WebLogic Plugin Enabled** check box.
- Save and activate the changes.

8.6.3 Registering Oracle HTTP Server With WebLogic Server

Once an Oracle WebLogic domain is created, the Oracle web tier can be linked to the domain. The advantage of doing this is that the Oracle web tier can be managed and monitored using Oracle Enterprise Manager Fusion Middleware Control.

To associate the Oracle web tier with the WebLogic domain use the following commands:

```
WEBHOST1> cd ORACLE_BASE/admin/instance_name/bin

WEBHOST1> ./opmnctl registerinstance -adminHost ADMINVHN -adminPort 7001
-adminUsername weblogic
```

You must also run this command from WEBHOST2 for OHS2.

After registering Oracle HTTP Server, it should appear as a manageable target in the Oracle Enterprise Manager Console. To verify this, log in to the Enterprise Manager Console. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

8.6.4 Setting the Frontend URL for the Administration Console and Setting Redirection Preferences

When you access the Oracle WebLogic Server Administration Console using a load balancer, changing the Administration Server's frontend URL is required so that the user's browser is redirected to the appropriate load balancer address.

The Oracle WebLogic Server Administration Console application tracks changes 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.

To change the Administration Server's frontend URL:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Expand the Environment node in the Domain Structure window.
4. Click **Servers** to open the Summary of Servers page.
5. Select **Admin Server** in the Names column of the table. The Settings page for AdminServer(admin) appears.
6. Click the **Protocols** tab.
7. Click the **HTTP** tab.
8. Set the **Frontend Host** to `admin.mycompany.com` and the **Frontend HTTP Port** to 80 (modify accordingly if HTTPS is used for the admin URL).
9. Save and activate the changes.
10. Disable tracking on configuration changes in the Oracle WebLogic Server Administration Console so that the console does not trigger the reload of configuration pages when activation of changes occurs.
 - a. Log in to the Oracle WebLogic Server Administration Console.
 - b. Click the **preferences** link in the banner.

- c. Click the **shared preferences** tab.
- d. Deselect the **follow configuration changes** check box.

Note: If you have any issues activating any configuration changes after modifying the Frontend Host and Port settings, then refer to [Section 16.8.2, "Redirecting of Users to Login Screen After Activating Changes in Administration Console."](#)

8.6.5 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as **Running** in the Admin 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

Validate WSM-PM_Cluster through both Oracle HTTP Servers using the following URLs:

- <http://WEBHOST1:7777/wsm-pm>
- <http://WEBHOST2:7777/wsm-pm>
- <http://WEBHOST1:7777/console>
- <http://WEBHOST2:7777/console>
- <http://WEBHOST1:7777/em>
- <http://WEBHOST2:7777/em>
- <https://wcp.mycompany.com/wsm-pm>
- <http://admin.mycompany.com/console>
- <http://admin.mycompany.com/em>

After setting the frontend URL to the load balancer address, access to the console through the WEBHOSTn addresses will be redirected by the console to the frontend URL, thus validating the correct configuration of both Oracle HTTP Server and the load balancer.

For information on configuring system access through the load balancer, see [Section 3.3, "Configuring the Load Balancer."](#)

After the registering Oracle HTTP Server as described in [Section 8.6.3, "Registering Oracle HTTP Server With WebLogic Server,"](#) the Oracle HTTP Server should appear as a manageable target in the Oracle Enterprise Manager Console. To verify this, log into the Enterprise Manager Console. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

8.6.6 Manually Failing Over the Administration Server to SOAHOST2

In case a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from SOAHOST1 to SOAHOST2.

Assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on ANY address. See step 14 in [Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain"](#).
- These procedures assume that the two nodes use two individual domain directories, and that the directories reside in local storage or in shared storage in different volumes.
- The Administration Server is failed over from SOAHOST1 to SOAHOST2, and the two nodes have these IPs:
 - SOAHOST1: 100.200.140.165
 - SOAHOST2: 100.200.140.205
 - ADMINVHN: 100.200.140.206. This is the VIP where the Administration Server is running, assigned to ethX:Y, available in SOAHOST1 and SOAHOST2.
- The domain directory where the Administration Server is running in SOAHOST1 is on a shared storage and is mounted also from SOAHOST2.
- Oracle WebLogic Server and Oracle Fusion Middleware components have been installed in SOAHOST2 as described in [Section 6, "Installing the Software for an Enterprise Deployment"](#) (that is, the same paths for ORACLE_HOME and MW_HOME that exist on SOAHOST1 are also available on SOAHOST2).

The following procedure shows how to fail over the Administration Server to a different node (SOAHOST2), but the Administration Server will still use the same WebLogic Server machine (which is a logical machine, not a physical machine).

To fail over the Administration Server to SOAHOST2:

1. Stop the Administration Server.
2. Migrate IP to the second node.
 - a. Run the following command as root on SOAHOST1 (where X:Y is the current interface used by ADMINVHN):

```
/sbin/ifconfig ethX:Y down
```

- b. Run the following command on SOAHOST2:

```
/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 to match the available network configuration in SOAHOST2.

3. Update routing tables through `arping`, for example:


```
SOAHOST2> /sbin/arping -b -A -c 3 -I eth0 10.0.0.1
```
4. Start the Administration Server on SOAHOST2 using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)
5. Test that you can access the Administration Server on SOAHOST2 as follows:
 - a. Ensure that you can access the Oracle WebLogic Server Administration Console using the following URL:

`http://ADMINVHN:7001/console`

- b. Check that you can access and verify the status of components in the Oracle Enterprise Manager using the following URL:

`http://ADMINVHN:7001/em`

Note: The Administration Server does not use Node Manager for failover. After a manual failover, the machine name that appears in the **Current Machine** field in the Administration Console for the server is SOAHOST1, and not the failover machine, SOAHOST2. Since Node Manager does not monitor the Administration Server, the machine name that appears in the **Current Machine** field, is not relevant and you can ignore it.

8.6.7 Validating Access to SOAHOST2 Through Oracle HTTP Server

Perform the same steps as in [Section 8.6.5, "Validating Access Through Oracle HTTP Server"](#). This is to check that you can access the Administration Server when it is running on SOAHOST2.

8.6.8 Failing the Administration Server Back to SOAHOST1

This step checks that you can fail back the Administration Server, that is, stop it on SOAHOST2 and run it on SOAHOST1 by migrating ADMINVHN back to SOAHOST1 node.

To migrate ADMINVHN back to SOAHOST1:

1. Make sure the Administration Server is not running.
2. Run the following command on SOAHOST2.

```
/sbin/ifconfig ethZ:N down
```

3. Run the following command on SOAHOST1:

```
/sbin/ifconfig ethX:Y 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 SOAHOST1

4. Update routing tables through arping. Run the following command from SOAHOST1.

```
/sbin/arping -b -A -c 3 -I ethZ 100.200.140.206
```

5. Start the Administration Server again on SOAHOST1 using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

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

6. Test that you can access the Oracle WebLogic Server Administration Console using the following URL:

`http://ADMINVHN:7001/console`

7. Check that you can access and verify the status of components in the Oracle Enterprise Manager using the following URL:

`http://ADMINVHN:7001/em`

8.7 Backing Up the WebLogic Domain Configuration

Perform a backup to save your domain configuration. Make sure you stop the server first. The configuration files are located in the following directory:

`ORACLE_BASE/admin/domain_name`

To back up the domain configuration, run the following command on SOAHOST1:

```
tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Back up the Instance Home on the web tier using the following command:

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

Extending the Domain for SOA Components

This chapter describes how to use the Configuration Wizard to extend the domain to include SOA components. You created in the domain in [Chapter 8, "Creating a Domain for an Enterprise Deployment."](#)

Note: Before starting the setup process, read the *Oracle Fusion Middleware Release Notes* for additional installation and deployment information.

Note: Follow the steps in this chapter only if you want to run SOA components on SOAHOST1 and SOAHOST2. If you do not want to run SOA components in your WebCenter Portal topology, you can skip this chapter.

This chapter contains the following sections:

- [Section 9.1, "Overview of Extending the Domain for SOA Components"](#)
- [Section 9.2, "Preparing to Extend the Domain for Oracle SOA Components"](#)
- [Section 9.3, "Extending the Domain for SOA Components using the Configuration Wizard"](#)
- [Section 9.4, "Configuring Oracle Coherence for Deploying Composites"](#)
- [Section 9.5, "Post-Configuration and Verification Tasks"](#)
- [Section 9.6, "Propagating the Domain Configuration to SOAHOST2"](#)
- [Section 9.7, "Configuring Oracle HTTP Server with the Extended Domain"](#)
- [Section 9.8, "Configuring a Default Persistence Store for Transaction Recovery"](#)
- [Section 9.9, "Configuring Oracle Adapters"](#)
- [Section 9.10, "Backing Up the SOA Configuration"](#)

9.1 Overview of Extending the Domain for SOA Components

Extend the WebLogic domain to include Oracle SOA components. [Table 9–1](#) lists the steps for configuring Oracle SOA and other tasks required for extending the domain for Oracle SOA components.

Table 9–1 Steps for Extending the Domain for SOA Components

Step	Description	More Information
Prepare for extending the Domain for SOA Components	Enable a VIP mapping for each of the hostnames.	Section 9.2.1, "Enabling VIP2 on SOAHOST1 and VIP3 on SOAHOST2"
Extend the Domain for SOA Components	Extend the WebLogic domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment" .	Section 9.3, "Extending the Domain for SOA Components using the Configuration Wizard"
Configure Oracle Coherence for Deploying Composites	Configure Oracle Coherence in order to use unicast communication for deploying composites.	Section 9.4, "Configuring Oracle Coherence for Deploying Composites"
Post-Configuration and Verification Tasks	Follow these instructions for post-configuration and validation tasks.	Section 9.5, "Post-Configuration and Verification Tasks"
Propagate the Domain Configuration to SOAHOST1	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory.	Section 9.5.3, "Propagating the Domain Changes to the Managed Server Domain Directory"
Configure the Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the managed servers, validate access, set the frontend HTTP host and port, and set the WLS Cluster address for the SOA_Cluster.	Section 9.7, "Configuring Oracle HTTP Server with the Extended Domain"
Configure a Default Persistence Store	Configure a default persistence store for transaction recovery.	Section 9.8, "Configuring a Default Persistence Store for Transaction Recovery"
Configure Oracle Adapters	Enable high availability for Oracle File and FTP Adapters, enable high availability for Oracle JMS Adapters, and scale the Oracle Database Adapter.	Section 9.9, "Configuring Oracle Adapters"
Back Up the SOA Configuration	Back up the newly extended domain configuration.	Section 9.10, "Backing Up the SOA Configuration"

9.2 Preparing to Extend the Domain for Oracle SOA Components

Before you run the Configuration Wizard to extend the domain, enable a VIP mapping for each of the hostnames on the two SOA machines

This section includes the following topics:

- [Section 9.2.1, "Enabling VIP2 on SOAHOST1 and VIP3 on SOAHOST2"](#)

9.2.1 Enabling VIP2 on SOAHOST1 and VIP3 on SOAHOST2

The SOA domain uses virtual hostnames as the listen addresses for the SOA managed servers. You must enable a VIP mapping each of these hostnames on the two SOA Machines, (VIP2 on SOAHOST1 and VIP3 on SOAHOST2), and must be correctly resolve the virtual hostnames in the network system used by the topology (either by DNS Server, hosts resolution).

To enable the VIP, follow the steps described in [Section 8.2, "Enabling VIP1 in SOAHOST1."](#) These VIPs and VHNs are required to enable server migration for the SOA Servers. Server migration must be configured for the SOA System for high

availability purposes. Refer to Chapter 9, "Server Migration" of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for more details on configuring server migration for the SOA servers.

9.3 Extending the Domain for SOA Components using the Configuration Wizard

Use the Configuration Wizard to extend the domain created in [Chapter 8, "Creating a Domain for an Enterprise Deployment"](#) to contain SOA components.

In this section we assume that the SOA deployment uses the same database service (wcpedg.mycompany.com) as the WebCenter Portal deployment. However, a deployment may choose to use a different database service specifically for SOA such as soaedg.mycompany.com.

Note: If you have not backed up the domain created in [Chapter 8, "Creating a Domain for an Enterprise Deployment"](#) back up the current domain before extending it for SOA components. You may use the backup to recover in case any errors are made in the domain extension. See "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain using the Configuration Wizard:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, Oracle recommends that all instances are running, so that the validation check later on becomes more reliable.
2. Shut down all managed servers in the domain.
3. Change directory to the location of the Configuration Wizard. This is within the Oracle Common home directory (notice that domain extensions are run from SOAHOST1 where the Administration Server resides).

```
cd ORACLE_COMMON_HOME/common/bin
```

4. Start the Configuration Wizard.

```
./config.sh
```

5. In the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.
6. In the WebLogic Domain Directory screen, select the WebLogic domain directory:

```
ORACLE_BASE/admin/domain_name/aserver/domain_name
```

Click **Next**.

7. In the Select Extension Source screen, do the following:
 - Select **Extend my domain automatically to support the following added products**.
 - Select the following products:
 - **Oracle SOA Suite 11.1.1.0**

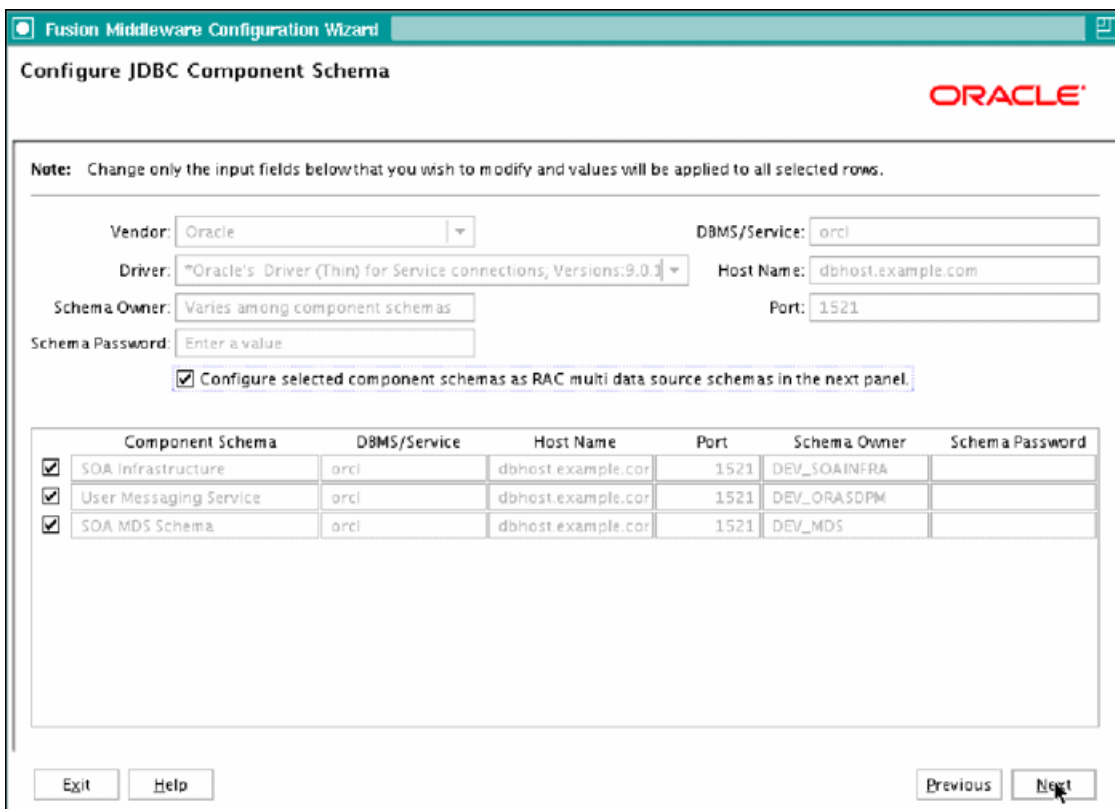
The following products should already be selected, and grayed out. They were selected when you created in domain in [Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain."](#)

- Basic WebLogic Server Domain
- Oracle Enterprise Manager
- Oracle WSM Policy Manager
- Oracle JRF

Click **Next**.

8. If you get a "Conflict Detected" message that Oracle JRF is already defined in the domain, select the **Keep Existing Component** option and click **OK**.
9. In the Configure JDBC Component Schema screen ([Figure 9-1](#)), do the following:
 - a. Select the **SOA Infrastructure**, **User Messaging Service**, and **SOA MDS Schema** rows in the table.
 - b. Select **Configure selected component schemas as RAC multi data source schemas in the next panel**.
 - c. Click **Next**.

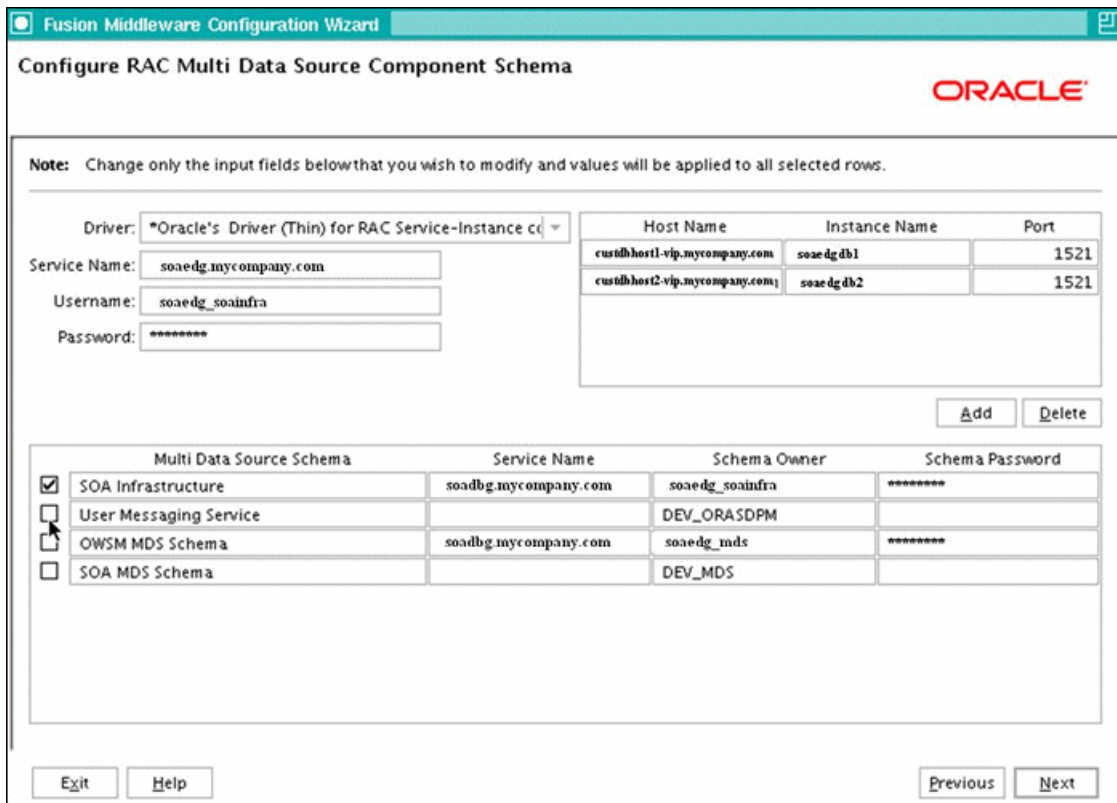
Figure 9-1 Configure JDBC Component Schema Screen



10. In the Configure RAC Multi Data Source Component Schema screen ([Figure 9-2](#)), do the following:
 - a. Select **SOA Infrastructure**.

- b. Enter values for the following fields, specifying the connect information for the RAC database that was seeded with RCU.
 - **Driver:** Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, 11.**
 - **Service Name:** Enter the service name of the database; for example, `wcpedg.mycompany.com`.
 - **Username:** Enter the complete user name (including prefix) for the schemas. The user names shown in [Figure 9-2](#) assume that `soedg` was used as prefix for schema creation from RCU.
 - **Password:** Enter the password to use to access the schemas.
- c. Click **Add** and enter the details for the first RAC instance.
- d. Repeat for each RAC instance.
- e. Deselect **SOA Infrastructure**.
- f. Select **User Messaging Service**.
- g. Repeat steps b, c, and d for the User Messaging Schema.
- h. Deselect **User Messaging Service**.
- i. Select **SOA MDS Schema**.
- j. Repeat steps b, c, and d for the SOA MDS Schema.
- k. Leave the OWSM MDS Schema information as it is.
- l. Click **Next**

Figure 9-2 Configure RAC Multi Data Source Component Schema Screen



11. In the Test JDBC Data Sources screen, the connections should be tested automatically. The Status column displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen and correct your entries.

Click **Next** when all the connections are successful.

12. In the Select Optional Configuration screen, select the following:

- JMS Distributed Destinations
- Managed Servers, Clusters, and Machines
- Deployments and Services
- JMS File Store

Click **Next**.

13. In the Select JMS Distributed Destination Type screen:

- Select **UDD** from the drop down list for UMSJMSYSTEMResource.
- Select **UDD** from the drop down list for SOAJMSModule.

14. In the Configure Managed Servers screen, add the required managed servers.

A server called `soa_server1` is created automatically. Rename this to `WLS_SOA1` and give it the attributes listed in [Table 9-2](#). Then, add a new server called `WLS_SOA2`. The `WLS_WSM1` and `WLS_WSM2` managed servers should already be present because they are part of the domain that you are extending. In the end, the list of managed servers should match that in [Table 9-2](#).

Table 9-2 Managed Servers

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_SOA1	SOAHOST1VHN1	8001	n/a	No
WLS_SOA2	SOAHOST2VHN1	8001	n/a	No
WLS_WSM1	SOAHOST1	7010	n/a	No
WLS_WSM2	SOAHOST2	7010	n/a	No

Click **Next**.

15. In the Configure Clusters screen, add the following clusters:

Table 9-3 Clusters

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
SOA_Cluster	unicast	n/a	n/a	SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
WSM-PM_Cluster	unicast	n/a	n/a	Leave it empty.

Click **Next**.

16. In the Assign Servers to Clusters screen, assign servers to clusters as follows:

- **SOA_Cluster:**
 - `WLS_SOA1`

- WLS_SOA2
- **WSM-PM_Cluster:**
 - WLS_WSM1
 - WLS_WSM2

Click **Next**.

17. In the Configure Machines screen, do the following:

- Delete the **LocalMachine** that appears by default.
- Click the **Unix Machine** tab. The following entries appear (listed in [Table 9–4](#)):

Table 9–4 Machines

Name	Node Manager Listen Address
SOAHOST1	SOAHOST1
SOAHOST2	SOAHOST2
ADMINHOST	localhost

Leave all other fields to their default values.

Click **Next**.

18. In the Assign Servers to Machines screen, assign servers to machines as follows:

- **ADMINHOST:**
 - AdminServer
- **SOAHOST1:**
 - WLS_SOA1
 - WLS_WSM1
- **SOAHOST2:**
 - WLS_SOA2
 - WLS_WSM2

Click **Next**.

19. In the Target Deployments to Clusters or Servers screen, ensure the following targets:

- **usermessagingserver** and **usermessagingdriver-email** should be targeted only to **SOA_Cluster**. (The **usermessaging-xmpp**, **usermessaging-smpp**, and **usermessaging-voicexml** applications are optional.)
- The **oracle.sdp.***, and **oracle.soa.*** libraries should be targeted only to **SOA_Cluster**.
- The **oracle.rules.*** library should be targeted only to **Admin Server** and **SOA_Cluster**.
- The **wsm-pm** application should be targeted only to **WSM-PM_Cluster**.
- The **oracle.wsm.seedpolicies** library should be targeted only to **WSM-PM_Cluster**.

Target this library to the **SOA_Cluster** also only if you are planning to deploy WebLogic WebServices to it.

Click **Next**.

20. In the Target Services to Clusters or Servers screen, ensure the following targets:
 - Target **mds-owsm**, **mds-owsm-rac0**, and **mds-owsm-rac1** to both **WSM-PM_Cluster** and **AdminServer**.

Click **Next**.

21. In the Configure JMS File Stores screen, enter the shared directory location specified for your JMS stores as recommended in [Section 4.3, "About Recommended Locations for the Different Directories"](#). For example:

```
ORACLE_BASE/admin/domain_name/soa_cluster_name/jms
```

Click **Next**.

22. In the Configuration Summary screen click **Extend**.

Note: Click **OK** to dismiss the warning dialog about the domain configuration ports conflicting with the host ports. This warning appears because of the existing WSM-PM installation.

23. In the Extending Domain screen, click **Done**.

You must start the Administration Server for this configuration to take effect.

24. Start the Administration Server using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

9.4 Configuring Oracle Coherence for Deploying Composites

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

Note: An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

9.4.1 Enabling Communication for Deployment Using Unicast Communication

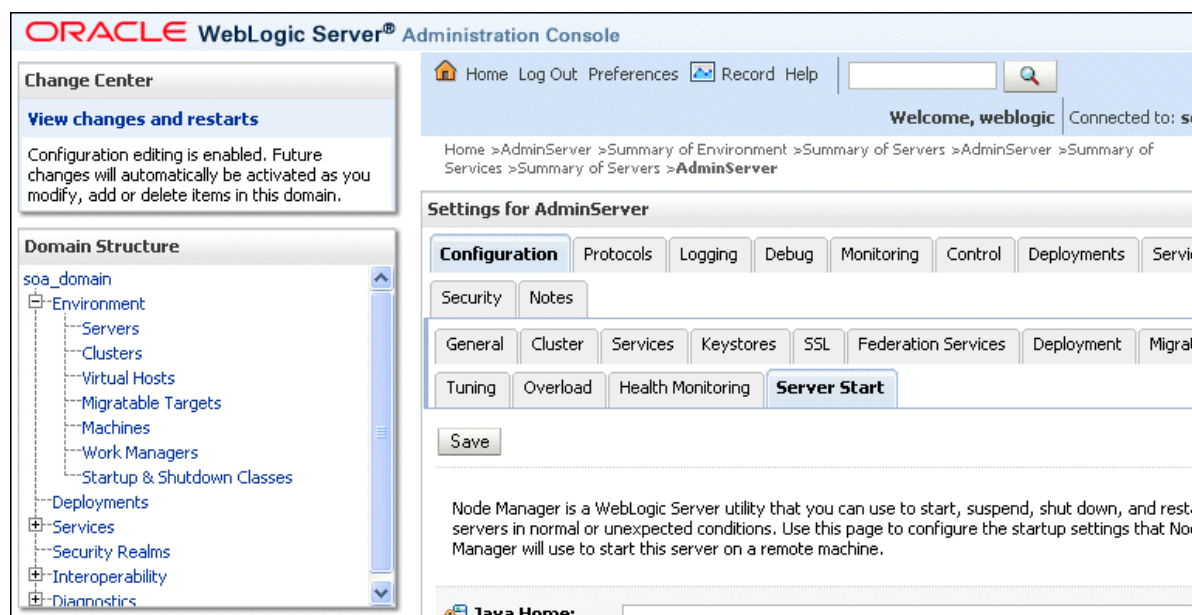
Specify the nodes using the `tangosol.coherence.wka<n>` system property, where `<n>` is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the

tangosol.coherence.localhost system property. This local host name should be the virtual host name used by the SOA server as the listener addresses (SOAHOST1VHN1 and SOAHOST2VHN1). Set this property by adding the -Dtangosol.coherence.localhost parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab (Figure 9-3).

Tip: To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

Note: SOAHOST1VHN1 is the virtual host name that maps to the virtual IP where WLS_SOA1 listening (in SOAHOST1). SOAHOST2VHN1 is the virtual host name that maps to the virtual IP where WLS_SOA2 is listening (in SOAHOST2).

Figure 9-3 Setting the Host Name Using the Start Server Tab of Oracle WebLogic Server Administration Console



9.4.2 Specifying the Host Name Used by Oracle Coherence

To add the host name used by Oracle Coherence, complete these steps:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (**WLS_SOA1** or **WLS_SOA2**, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab (illustrated in Figure 9-3).
7. Enter the following for WLS_SOA1 and WLS_SOA2 into the Arguments field.

Note: There should be no breaks in lines between the different -D parameters. Do not copy or paste the text from above to your Administration Console's arguments text field. This may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN1  
-Dtangosol.coherence.wka2=SOAHOST2VHN1  
-Dtangosol.coherence.localhost=SOAHOST1VHN1  
-Dtangosol.coherence.localport=8089  
-Dtangosol.coherence.wka1.port=8089  
-Dtangosol.coherence.wka2.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN1  
-Dtangosol.coherence.wka2=SOAHOST2VHN1  
-Dtangosol.coherence.localhost=SOAHOST2VHN1  
-Dtangosol.coherence.localport=8089  
-Dtangosol.coherence.wka1.port=8089  
-Dtangosol.coherence.wka2.port=8089
```

For more information about Coherence Clusters see the *Oracle Coherence Developer's Guide*.

For WLS_SOA1, enter the following:

```
-Dtangosol.coherence.wka1=SOAHOST1VHN1  
-Dtangosol.coherence.wka2=SOAHOST2VHN1  
-Dtangosol.coherence.localhost=SOAHOST1VHN1
```

For WLS_SOA2, enter the following:

```
-Dtangosol.coherence.wka1=SOAHOST2VHN1  
-Dtangosol.coherence.wka2=SOAHOST1VHN1  
-Dtangosol.coherence.localhost=SOAHOST2VHN1
```

8. Click **Save** and **Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

9.5 Post-Configuration and Verification Tasks

After extending the domain with the configuration Wizard and configuring Oracle Coherence, follow these instructions for post-configuration and validation.

This section includes the following topics:

- [Section 9.5.1, "Disabling Host Name Verification for the WLS_SOAn Managed Server"](#)
- [Section 9.5.2, "Restarting the Node Manager on SOAHOST1"](#)
- [Section 9.5.3, "Propagating the Domain Changes to the Managed Server Domain Directory"](#)
- [Section 9.5.4, "Starting and Validating the WLS_SOA1 Managed Server"](#)

9.5.1 Disabling Host Name Verification for the WLS_SOAn Managed Server

For the enterprise deployment described in this guide, you set up the appropriate certificates to authenticate the different nodes with the Administration Server after you have completed the procedures to extend the domain for Oracle SOA. Therefore, you must disable the host name verification for the WLS_SOAn managed server to avoid errors when managing the different WebLogic Servers. You enable host name verification again once the Enterprise Deployment topology configuration is complete. See [Section 11.5, "Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2"](#) for more information.

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page appears.
5. Select **WLS_SOA1** (represented as a hyperlink) from the Names column of the table. The Settings page appears.
6. Select the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set Hostname Verification to **None**.
9. Click **Save**.
10. Repeat these steps for the WLS_SOA2 managed server.
11. Save and activate the changes.
12. This change requires a restart of the Administration Server and Node Managers.

- a. To restart the Administration Server see [Chapter 8.4.3, "Starting the Administration Server on SOAHOST1."](#)
- b. To restart Node Manager on SOAHOST1, see [Chapter 9.5.2, "Restarting the Node Manager on SOAHOST1."](#)

Repeat for the Node Manager in SOAHOST2

9.5.2 Restarting the Node Manager on SOAHOST1

Use the `startNodeManager.sh` script to restart Node Manager.

To restart the Node Manager on SOAHOST1:

1. Stop Node Manager by stopping the process associated with it:
 - If it is running in the foreground in a shell, simply use CTRL+C.
 - If it is running in the background in the shell, find the associate process and use the `kill` command to stop it. For example:

```
ps -ef | grep NodeManager
orcl      9139  9120  0 Mar03 pts/6    00:00:00 /bin/sh
          ./startNodeManager.sh
```

```
kill -9 9139
```

2. Start Node Manager:

```
./startNodeManager.sh
```

9.5.3 Propagating the Domain Changes to the Managed Server Domain Directory

Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory.

To propagate start scripts and classpath configuration:

1. Create a copy of the managed server domain directory and the managed server applications directory.
2. Run the `pack` command on SOAHOST1 to create a template pack using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_
name
-template=soadomaintemplateExtSOA.jar -template_name=soa_domain_templateExtSOA
```

3. Run the `unpack` command on SOAHOST1 to unpack the propagated template to the domain directory of the managed server using the following command:

```
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-overwrite_domain=true -template=soadomaintemplateExtSOA.jar
-app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

Note: The `-overwrite_domain` option in the `unpack` command, allows unpacking a managed server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the managed server domain directory, they must be restored after this `unpack` operation.

9.5.4 Starting and Validating the WLS_SOA1 Managed Server

Start and validate the WLS_SOA1 managed server using the Administration Console.

To start the WLS_SOA1 managed server on SOAHOST1:

1. Start the WLS_SOA1 managed server using the Oracle WebLogic Server Administration Console as follows:
 - a. Access the Administration Console at the following URL:
`http://ADMINVHN:7001/console`

 ADMINVHN is the virtual host name that maps to the virtual IP where the Administration Server is listening (in SOAHOST1).
 - b. Expand the **Environment** node in the **Domain Structure** window.
 - c. Click **Servers**.
 The Summary of Servers screen appears.
 - d. Click the **Control** tab.
 - e. Select **WLS_SOA1** and then click **Start**.
2. Verify that the server status is reported as **Running**. 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

3. Access the following URL to verify status of WLS_SOA1:

`http://SOAHOST1VHN1:8001/soa-infra/`

Access the following URL to verify status of the worklist application:

`http://SOAHOST1VHN1:8001/integration/worklistapp/`

Access the following URL to verify status of the composer application:

`http://SOAHOST1VHN1:8001/soa/composer/`

Before verifying access is granted, ensure that the WLS_WSM1 managed server is up and running.

9.6 Propagating the Domain Configuration to SOAHOST2

After completing the configuration of SOAHOST1, propagate the configuration to SOAHOST2 using the `unpack` utility, and then validate the propagated configuration.

This section contains the following topics:

- [Section 9.6.1, "Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility"](#)
- [Section 9.6.2, "Starting and Validating the WLS_SOA2 Managed Server"](#)

9.6.1 Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility

Propagate the domain you just configured to SOAHOST2 using the unpack utility.

To propagate the domain configuration:

1. Run the following command on SOAHOST1 to copy the template file created in the previous step to SOAHOST2.

```
cd ORACLE_COMMON_HOME/common/bin

scp soadomaintemplateExtSOA.jar oracle@SOAHOST2:ORACLE_COMMON_HOME/common/bin
```

2. Run the unpack command on SOAHOST2 to unpack the propagated template.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh
-domain=ORACLE_BASE/admin/domain_name/msserver/domain_name/
-template=soadomaintemplateExtSOA.jar -overwrite_domain=true
-app_dir=ORACLE_BASE/admin/domain_name/msserver/applications
```

Note: The `-overwrite_domain` option in the unpack command, allows unpacking a managed server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the managed server domain directory, they must be restored after this unpack operation.

9.6.2 Starting and Validating the WLS_SOA2 Managed Server

Use the Administration Console to start the WLS_SOA2 managed server. Validate it by accessing soa-infra, and worklistapp URLs.

To start the WLS_SOA2 managed server and check that it is configured correctly:

1. Start the WLS_SOA2 managed server using the Administration Console.
2. Verify that the server status is reported as **Running** in the Admin 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.
3. Access the following URL for soa-infra:

```
http://SOAHOST2VHN1:8001/soa-infra
```

4. Access the following URL to verify status of the worklist application.

```
http://SOAHOST2VHN1:8001/integration/worklistapp/
```

Before verifying access is granted, ensure that at least one of the managed servers (WLS_WSM1 or WLS_WSM2) is up and running.

Note: Although the WLS_SOA1 server may be up, some applications may be in a failed state. Therefore, Oracle recommends verifying the URLs above and watch for errors pertaining each individual application in the server's output file.

5. Access the following URL to verify status of the composer application.

`http://SOAHOST2VHN1:8001/soa/composer/`

9.7 Configuring Oracle HTTP Server with the Extended Domain

After propagating the domain configuration to SOAHOST2, configure the Oracle HTTP Server with the extended domain.

This section includes the following topics:

- [Section 9.7.1, "Configuring Oracle HTTP Server for the WLS_SOA \$n\$ Managed Servers"](#)
- [Section 9.7.2, "Validating Access Through Oracle HTTP Server"](#)
- [Section 9.7.3, "Setting the Frontend HTTP Host and Port"](#)

9.7.1 Configuring Oracle HTTP Server for the WLS_SOA n Managed Servers

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

Sample scenarios:

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

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

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

To enable Oracle HTTP Server to route to the SOA_Cluster, which contains the WLS_SOA n managed servers, set the `WebLogicCluster` parameter to the list of nodes in the cluster.

The entry for `/workflow` is optional. It is for workflow tasks associated with Oracle ADF task forms. The `/workflow` URL itself can be a different value, depending on the form.

To enable Oracle HTTP Server to route to the SOA_Cluster:

1. On WEBHOST1 and WEBHOST2, add the following lines to the `ORACLE_BASE/admin/instance_name/config/OHS/component_name/mod_wl_ohs.conf` file:

```
# SOA soa-infra app
<Location /soa-infra>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Worklist
<Location /integration>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Workflow
<Location /workflow>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# UMS WS
<Location /ucs/messaging/webservice>
    SetHandler weblogic-handler
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

```
#Required if attachments are added for workflow tasks
<Location /ADFAttachmentHelper>
  SetHandler weblogic-handler
  WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

# SOA composer application
<Location /soa/composer>
  SetHandler weblogic-handler
  WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
```

2. Restart Oracle HTTP Server on WEBHOST1 and WEBHOST2:

```
WEBHOST1> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs1
WEBHOST2> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs2
```

9.7.2 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as **Running** in the Admin 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

Verify that you can access these URLs, where 'webhostN' specifies the name of each Oracle HTTP Server host (for example, WEBHOST1, WEBHOST2):

- `http://webhostN:7777/soa-infra`
- `http://webhostN:7777/integration/worklistapp`
- `http://webhostN:7777/sdpMessaging/userprefs-ui`
- `http://webhostN:7777/soa/composer`

Validate SOA_Cluster through both Oracle HTTP Server instances.

For information on configuring system access through the load balancer, see [Section 3.3, "Configuring the Load Balancer."](#)

9.7.3 Setting the Frontend HTTP Host and Port

Set the frontend HTTP host and port using the Administration Console, and then restart the server.

To set the frontend HTTP host and port for the Oracle WebLogic Server cluster:

1. In the WebLogic Server Administration Console, in the Change Center section, click **Lock & Edit**.
2. In the left pane, choose **Environment** in the Domain Structure window and then choose **Clusters**. The Summary of Clusters page appears.
3. Select the **SOA_Cluster** cluster.
4. Select **HTTP**.

5. Set the values for the following:
 - **Frontend Host:** wcp.mycompany.com
 - **Frontend HTTPS Port:** 443
 - **Frontend HTTP Port:** 80
6. Click **Save**.
7. To activate the changes, click **Activate Changes** in the Change Center section of the Administration Console.
8. Restart the servers to make the Frontend Host directive in the cluster effective.

Note: When HTTPS is enabled in the load balancer and the load balancer terminates SSL (the SOA servers receive only HTTP requests, not HTTPS), as suggested in this guide, the endpoint protocol for webservices is set to `http`. Since the load balancer redirects HTTP to HTTPS this causes the following exception when testing webservices functionality in Oracle Enterprise Manger Fusion Middleware Control:

```
(javax.xml.soap.SOAPException:  
oracle.j2ee.ws.saaj.ContentTypeException)
```

To resolve this exception, update the URL endpoint:

In the Enterprise Manager Test Page, check **Edit Endpoint URL**.

Within the endpoint URL page:

- Change `http` to `https`.
 - Change the default port number (say 80) to SSL port (say 443).
-

Callback URL

The SOA system calculates the callback URL as follows:

- If a request to SOA originates from an external or internal service, then SOA uses the callback URL specified by the client.
- If a request to an external or internal asynchronous service originates from SOA, the callback URL is determined using the following method, in decreasing order of preference:
 1. Use `callbackServerURL` specified as a binding property for the specific reference. (You can set this when modeling the composite or at runtime using the MBeans). This allows different service calls to have different callback URLs. That is, a callback URL from an external service can be set to be different than one to an internal service In the context of the Enterprise Deployment architecture, typically this will be `wcp.mycompany.com (443/https)` for external services and `wcpinternal.mycompany.com (7777/http)` for internal services. At runtime, this property is set using the System MBean Browser, through the corresponding binding mbean. To add a specific URL, add a `callbackServerURL` property to its Properties attribute, then invoke the save operation.
 2. Use the callback URL as specified in `soa-infra-config.xml`. In this case, only one address can be specified. When a mix of both external and internal services can be invoked, this should be set to `wcp.mycompany.com (443/https)` in the

Enterprise Deployment architecture. When only internal services are to be invoked, this can be set to `wcpinternal.mycompany.com (7777/http)`.

3. Use the callback URL as the frontend host specified in WLS for the SOA_Cluster. In this case, too, only one address can be specified and the recommendation is same as the one for *soa-infra-config.xml*.
4. Use the local host name as provided by WLS MBean APIs. This is not recommended in HA environments such as Enterprise Deployment.

9.8 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may 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 a dual-ported SCSI disk or on a Storage Area Network (SAN).

To set the location for the default persistence store, complete these steps:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Change Center section, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node. The Summary of Servers page appears.
4. Click the name of the server (represented as a hyperlink) in Name column of the table. The settings page for the selected server appears and defaults to the Configuration tab.
5. Click the **Services** tab.
6. 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:


```
ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs
```
7. Click **Save**.
8. Verify that the following files are created in the `ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs` directory after WLS_SOA1 and WLS_SOA2 are restarted:
 - `_WLS_WLS_SOA1000000.DAT`
 - `_WLS_WLS_SOA2000000.DAT`

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. Both WLS_SOA1 and WLS_SOA2 must be able to access this directory. This directory must also exist before you restart the server.

9.9 Configuring Oracle Adapters

Configure Oracle File, FTP, and database adapters for the extended SOA domain.

This section includes the following topics:

- [Section 9.9.1, "Enabling High Availability for Oracle File and FTP Adapters."](#)
- [Section 9.9.2, "Enabling High Availability for Oracle JMS Adapter."](#)
- [Section 9.9.3, "Scaling the Oracle Database Adapter."](#)

9.9.1 Enabling High Availability for Oracle File and FTP Adapters

The Oracle File and FTP Adapters enable a BPEL process or an Oracle Mediator to read and write files on local file systems and on remote file systems through FTP (File Transfer Protocol). These adapters support high availability for an active-active topology with Oracle BPEL Process Manager and Oracle Mediator service engines for both inbound and outbound operations. To make Oracle File and FTP Adapters highly available for outbound operations, use the database mutex locking operation as described in "High Availability in Outbound Operations" in *Oracle Fusion Middleware User's Guide for Technology Adapters*. The database mutex locking operation enables these adapters to ensure that multiple references do not overwrite one another if they write to the same directory.

Note: The operation described above is necessary only if your application requires these adapters.

Note: The File Adapter picks up a file from the inbound directory, processes it, and then outputs a file to the output directory. Because the File Adapter is non-transactional, files can be processed twice. As a result, it is possible to get duplicate files when there is failover in the RAC backend or in the SOA managed servers.

9.9.1.1 Using the Database Mutex Locking Operation

Use the following procedure to make an outbound Oracle File or FTP Adapter service highly available using database table as a coordinator:

Note: You must increase global transaction timeouts if you use database as a coordinator.

1. Create Database Tables

You are not required to perform this step since the database schemas are pre-created as a part of soainfra.

2. Modify Deployment Descriptor for Oracle File Adapter

Modify Oracle File Adapter deployment descriptor for the connection-instance corresponding to `eis/HFileAdapter` from the Oracle WebLogic Server console:

- a. Log into your Oracle WebLogic Server console. To access the console navigate to `http://servername:portnumber/console`.
- b. Click **Deployments** in the left pane for Domain Structure.

- c. Click **FileAdapter** under Summary of Deployments on the right pane.
- d. Click the **Configuration** tab.
- e. Click the **Outbound Connection Pools** tab, and expand **javax.resource.cci.ConnectionFactory** to see the configured connection factories.
- f. Click **eis/HFileAdapter**. The Outbound Connection Properties for the connection factory corresponding to high availability is displayed.
- g. The connection factory properties appear as shown in [Figure 9-4](#).

Figure 9-4 Oracle WebLogic Server Console - Settings for javax.resource.cci.Connectionfactory Page

Settings for javax.resource.cci.ConnectionFactory

General Properties Transaction Authentication Connection Pool Logging

This page allows you to view and modify the configuration properties of this outbound connection pool. Properties you modify here are saved to a deployment plan.

Outbound Connection Properties

Save Showing 1 to 4 of 4 Previous | Next

<input type="checkbox"/>	Property Name	Property Type	Property Value
<input type="checkbox"/>	controlDir	java.lang.String	/scratch/mycontroldir
<input type="checkbox"/>	inboundDataSource	java.lang.String	jdbc/SOADDataSource
<input type="checkbox"/>	outboundDataSource	java.lang.String	jdbc/SOADDataSource
<input type="checkbox"/>	outboundLockTypeForWrite	java.lang.String	oracle

Save Showing 1 to 4 of 4 Previous | Next

Click on **Lock and Edit**. After this, the property value column becomes editable (you can click on any of the rows under "Property Value" and modify its value).

The new parameters in connection factory for Oracle File and FTP Adapters are as follows:

controlDir: Set it to the directory structure where you want the control files to be stored. You must set it to a shared location if multiple WebLogic Server instances run in a cluster. Structure the directory for shared storage as follows:

```
ORACLE_BASE/admin/domain_name/cluster_name/fadapter
```

inboundDataSource: Set the value to jdbc/SOADDataSource. This is the data source, where the schemas corresponding to high availability are pre-created. The pre-created schemas can be found under ORACLE_HOME/rcu/integration/soainfra/sql/adapter/createschema_adapter_oracle.sql. If you want to create the schemas elsewhere, use this script. You must set the inboundDataSource property accordingly if you choose a different schema.

`outboundDataSource`: Set the value to `jdbc/SOADDataSource`. This is the data source where the schemas corresponding to high availability are pre-created. The pre-created schemas can be found under `ORACLE_HOME/rcu/integration/soainfra/sql/adapter/createschema_adapter_oracle.sql`. If you want to create the schemas elsewhere, use this script. You must set the `outboundDataSource` property if you choose to do so.

`outboundDataSourceLocal`: Set the value to `jdbc/SOALocalTxDataSource`. This is the datasource where the schemas corresponding to high availability are pre-created.

`outboundLockTypeForWrite`: Set the value to `oracle` if you are using Oracle Database. By default the Oracle File and FTP Adapters use an in-memory mutex to lock outbound write operations. You must choose from the following values for synchronizing write operations:

`memory`: The Oracle File and FTP Adapters use an in-memory mutex to synchronize access to the file system.

`oracle`: The adapter uses Oracle Database sequence.

`db`: The adapter uses a pre-created database table (`FILEADAPTER_MUTEX`) as the locking mechanism. You must use this option only if you are using a schema other than the Oracle Database schema.

`user-defined`: The adapter uses a user-defined mutex. To configure the user-defined mutex, you must implement the mutex interface: `"oracle.tip.adapter.file.Mutex"` and then configure a new binding-property with the name `"oracle.tip.adapter.file.mutex"` and value as the fully qualified class name for the mutex for the outbound reference.

- h. Click **Save** after you update the properties. The Save Deployment Plan page appears.
- i. Enter a shared storage location for the deployment plan. The directory structure is as follows:

```
ORACLE_BASE/admin/domain_name/cluster_name/dp/Plan.xml
```

- j. Click **Save and Activate**.
- k. Configure BPEL Process or Mediator Scenario to use the connection factory as shown in the following example (in the `jca` file included in the composite for the binding component):

```
<adapter-config name="FlatStructureOut"
  adapter="File Adapter"
  xmlns="http://platform.integration.oracle/blocks/adapter/fw/metadata">
  <connection-factory location="eis/HAFileAdapter" adapterRef="" />
  <endpoint-interaction portType="Write_ptt" operation="Write">
<interaction-spec
  className="oracle.tip.adapter.file.outbound.FileInteractionSpec">
    <property ./>
    <property ./>
  </interaction-spec>
</endpoint-interaction>
</adapter-config>
```

Note: The location attribute is set to `eis/HAFileAdapter` for the connection factory.

9.9.2 Enabling High Availability for Oracle JMS Adapter

When the Oracle JMS adapter communicates with multiple servers in a cluster, the adapter's connection factory property `FactoryProperties` must list available servers. If it does not list servers, the connection establishes to only one random server. If that particular server goes down, no further messages are processed.

To verify that the adapter's JCA connection factory that you use, for example `eis/wls/Queue`, contains the required properties:

1. Log into your Oracle WebLogic Server console. To access the console, navigate to:

```
http://servername:portnumber/console
```

2. Click **Deployments** in the left pane for Domain Structure.
3. Click **JMSAdapter** under Summary of Deployments on the right pane.
4. Click the **Configuration** tab.
5. Click the **Outbound Connection Pools** tab and expand `oracle.tip.adapter.jms.IJmsConnectionFactory` to see the configured connection factories.
6. Click the specific instance you are using (for example, `eis/wls/Queue`). The **Outbound Connection Properties** for the connection factory opens.
7. Click **Lock & Edit**.
8. In the `FactoryProperties` field (click on the corresponding cell under **Property value**), enter the following:

```
java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory;
java.naming.provider.url=t3://soahostvhn1:8001,soahos2tvhn1:8001;java.naming.se
curity.principal=weblogic;
java.naming.security.credentials=weblogic1
```

9. Click **Enter**, save the changes, and then activate them.

Update the deployment in the console:

1. Click **Deployments** and select the JMS Adapter.
2. Click **Lock and Edit** then **Update**.
3. Select **Update this application in place with new deployment plan changes (A deployment plan must be specified for this option.)** and select the deployment plan saved in a shared storage location; all servers in the cluster must be able to access the plan).
4. Click **Finish** and activate the changes.

9.9.3 Scaling the Oracle Database Adapter

If you are using Logical Delete polling, and you set `MarkReservedValue`, skip locking is not used.

Formerly, the best practice for multiple Oracle Database Adapter process instances deployed to multiple Oracle BPEL Process Manager, or Oracle Mediator nodes was essentially using `LogicalDeletePollingStrategy` or `DeletePollingStrategy` with a unique `MarkReservedValue` on each polling node, and setting `MaxTransactionSize`.

However, with the introduction of skip locking in this release that approach has now been superseded. If you were using this approach previously, you can simply remove

(in `db.jca`) or clear (Logical Delete Page of wizard) the `MarkReservedValue`, and you automatically get skip locking.

The benefits of using skip locking over a reserved value include:

- Skip locking scales better in a cluster and under load.
- All work is in one transaction (as opposed to update/reserve, then commit, then select in a new transaction), so the risk of facing a non-recoverable situation in a high availability environment is minimized.
- No unique `MarkReservedValue` must be specified. Previously, for this to work you would have to configure a complex variable, such as `R${weblogic.Name-2}-${IP-2}-${instance}`.

For more information, see "Scalability" and "Polling Strategies" in *Oracle Fusion Middleware User's Guide for Technology Adapters*.

9.10 Backing Up the SOA Configuration

After you have verified that the extended 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, the regular deployment-specific backup and recovery process can be initiated. The *Oracle Fusion Middleware Administrator's Guide* provides further details.

For information about backing up the environment, see "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*. For information about recovering your information, see "Recovering Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

To back up the domain configuration:

1. Back up the web tier:
 - a. Shut down the instance using `opmnctl`.


```
ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
```
 - 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 using `opmnctl`:


```
ORACLE_BASE/admin/instance_name/bin/opmnctl startall
```
2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or OS tools such as `tar` for cold backups if possible.
3. Back up the Administration Server domain directory to save your domain configuration. The configuration files are located in the following directory:

```
ORACLE_BASE/admin/domain_name
```

To back up the Administration Server run the following command on SOAHOST1:

```
tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Extending the Domain for WebCenter Portal Components

This chapter describes how to use the Configuration Wizard to extend the domain you created in [Chapter 8, "Creating a Domain for an Enterprise Deployment"](#) to include WebCenter Portal components.

Note: Before starting the setup process, read the *Oracle Fusion Middleware Release Notes* for additional installation and deployment information.

This chapter contains the following sections:

- [Section 10.1, "Overview of Extending the Domain for WebCenter Portal Components"](#)
- [Section 10.2, "Extending the Domain for WebCenter Portal Components using the Configuration Wizard"](#)
- [Section 10.3, "Post-Configuration Tasks"](#)
- [Section 10.4, "Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2"](#)
- [Section 10.5, "Configuring the Java Object Cache for Spaces_Cluster"](#)
- [Section 10.6, "Converting Discussions from Multicast to Unicast"](#)
- [Section 10.7, "Configuring Clustering on the Discussions Server"](#)
- [Section 10.8, "Configuring Analytics"](#)
- [Section 10.9, "Configuring Activity Graph"](#)
- [Section 10.10, "Configuring REST APIs"](#)
- [Section 10.11, "Configuring Oracle HTTP Server with the Extended Domain"](#)
- [Section 10.12, "Backing Up the WebCenter Portal Configuration"](#)

10.1 Overview of Extending the Domain for WebCenter Portal Components

Extend the WebLogic domain to include Oracle WebCenter Portal components. [Table 10-1](#) lists the steps for configuring WebCenter Portal and other tasks required for extending the domain for WebCenter Portal components.

Table 10–1 Steps for Extending the Domain for WebCenter Portal Components

Step	Description	More Information
Extend the domain for WebCenter Portal components	Extend the WebLogic domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment" .	Section 10.2, "Extending the Domain for WebCenter Portal Components using the Configuration Wizard"
Disable host name verification for WebCenter Portal managed servers	Disable host name verification.	Section 10.3.1, "Disabling Host Name Verification for the WebCenter Portal Managed Servers"
Perform post-configuration tasks	Follow these instructions for post-configuration tasks.	Section 10.3, "Post-Configuration Tasks"
Propagate the domain configuration to the Managed Server domain directory	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory.	Section 10.3.3, "Propagating the Domain Changes to the Managed Server Domain Directory"
Propagate the domain configuration to SOAHOST2, WCPHOST1, WCPHOST2	Propagate the domain configuration to all other managed servers.	Section 10.4.1, "Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2 Using the unpack Utility"
Configure Java object caching	Configure the Java Object Cache to increase the performance of the Spaces application.	Section 10.5, "Configuring the Java Object Cache for Spaces_Cluster"
Configure WebCenter Portal services	Configure Discussions, Analytics, Activity Graph, and REST API services.	Section 10.6, "Converting Discussions from Multicast to Unicast" Section 10.7, "Configuring Clustering on the Discussions Server" Section 10.8, "Configuring Analytics" Section 10.9, "Configuring Activity Graph" Section 10.10, "Configuring REST APIs"
Configure the Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the managed servers, and validate access.	Section 10.11.1, "Configuring Oracle HTTP Server for the WC_Spacesn, WC_Portletn, WC_Utilitesn, and WC_Collaborationn Managed Servers"
Back Up the WebCenter Portal Configuration	Back up the newly extended domain configuration.	Section 10.12, "Backing Up the WebCenter Portal Configuration"

10.2 Extending the Domain for WebCenter Portal Components using the Configuration Wizard

Use the Configuration Wizard to extend the domain created in [Chapter 8, "Creating a Domain for an Enterprise Deployment"](#) to contain WebCenter Portal components.

Note: You must back up the current domain before extending the domain. You may use the backup to recover in case any errors are made in the domain extension. See "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain using the Configuration Wizard:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, Oracle recommends that all instances are running, so that the validation check later on becomes more reliable.

2. Shut down all managed servers in the domain.

3. Change directory to the location of the Configuration Wizard. This is within the Oracle Common home directory (notice that domain extensions are run from SOAHOST1 where the Administration Server resides).

```
cd ORACLE_COMMON_HOME/common/bin
```

4. Start the Configuration Wizard.

```
./config.sh
```

5. In the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.

6. In the WebLogic Domain Directory screen, select the WebLogic domain directory:

```
ORACLE_BASE/admin/domain_name/aserver/domain_name
```

Click **Next**.

7. In the Select Extension Source screen, do the following:

- Select **Extend my domain automatically to support the following added products**.

- Select the following products:

- **Oracle WebCenter Spaces**
- **Oracle WebCenter Services Portlets**
- **Oracle WebCenter Pagelet Producer**
- **Oracle Portlet Producers**
- **Oracle WebCenter Discussions Server**
- **Oracle WebCenter Activity Graph Engines**
- **Oracle WebCenter Personalization**
- **Oracle Webcenter Analytics Collector**

The following products should already be selected, and grayed out. They were selected when you created in domain in [Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain."](#)

- Basic WebLogic Server Domain
- Oracle JRF
- Oracle WSM Policy Manager

Click **Next**.

8. If you get a "Conflict Detected" message that Oracle JRF is already defined in the domain, select the **Keep Existing Component** option and click **OK**.

9. In the Configure JDBC Data Sources screen, do the following:

- a. Ensure that the following data sources appear on the screen. The user names shown in [Table 10-2](#) assume that `wcpedg` was used as prefix for schema creation from RCU.

Table 10–2 Values for Data Sources

Data Source	User Name
WebCenterDS Schema	wcpedg_webcenter
ActivitiesDS Schema	wcpedg_activities
DiscussionDS Schema	wcpedg_discussions
PersonalizationDS Schema	wcpedg_webcenter
PortletDS Schema	wcpedg_portlet
Portlet-ServicesProducerDS	wcpedg_portlet
WC-ServicesProducerDS	wcpedg_webcenter
WebCenterMDS Schema	wcpedg_mds
PersonalizationMDS Schema	wcpedg_mds
mds-PageletProducerDS Schema	wcpedg_mds
mds-ServicesProducerDS Schema	wcpedg_mds

- b. Select the check box next to all the component schemas.
 - c. Select **Configure all datasources as RAC multi-datasources in the next panel**.
 - d. Click **Next**.
10. In the Configure RAC Multi Data Sources Component Schema screen:
- a. Select first multi data source schema, **WebCenterDS Schema**.
 - b. Enter values for the following fields, specifying the connect information for the RAC database that was seeded with RCU.
 - **Driver:** Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, 11**.
 - **Service Name:** Enter the service name of the database, for example, `wcpedg.mycompany.com`.
 - **Username prefix:** Enter the complete user name (including prefix) for the schemas. The user names shown in [Table 10–2](#) assume that `wcpedg` was used as the prefix for schema creation from RCU.
 - **Password and Confirm Password:** Enter the password to use to access the schemas.
 - c. Click **Add** and enter the details for the first RAC instance.
 - d. Repeat for each RAC instance.
 - e. Deselect **WebCenterDS Schema**.
 - f. Select next data source schema, for example **ActivitiesDS Schema**, and repeat steps b, c, and d.
 - g. Repeat step f for all the multi data source schemas listed (see also [Table 10–2](#)).
 - h. Click **Next**.
11. In the Test JDBC Data Sources screen, the connections should be tested automatically. The **Status** column displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen and correct your entries.

Click **Next** when all the connections are successful.

12. In the Advanced Configuration Screen, select the following:

- Managed Servers, Clusters and Machines
- Deployments and Services

Click **Next**.

13. In the Configure Managed Servers screen, add the following managed servers (Table 10-3):

Table 10-3 Managed Servers

Name	Server	Listen Port	SSL Listen Port	SSL Enabled
WC_Spaces1	WCPHOST1	9000	n/a	No
WC_Spaces2	WCPHOST2	9000	n/a	No
WC_Portlet1	WCPHOST1	9001	n/a	No
WC_Portlet2	WCPHOST2	9001	n/a	No
WC_Collaboration1	WCPHOST1	9002	n/a	No
WC_Collaboration2	WCPHOST2	9002	n/a	No
WC_Uilities1	WCPHOST1	9003	n/a	No
WC_Uilities2	WCPHOST2	9003	n/a	No

Note: Managed Servers may be renamed but DO NOT remove any of the original Managed Servers on this page.

Note: Providing the listen address is mandatory if the cluster mode is 'unicast'.

Click **Next**.

14. In the Configure Clusters screen, add four new clusters (Table 10-4):

Note: WSM-PM_Cluster should already display in the list.

Table 10-4 Clusters

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
Spaces_Cluster	unicast	n/a	n/a	Leave it empty.
Portlet_Cluster	unicast	n/a	n/a	Leave it empty.
Collab_Cluster	unicast	n/a	n/a	Leave it empty.
Utilities_Cluster	unicast	n/a	n/a	Leave it empty.

Click **Next**.

15. In the Assign Servers to Clusters screen, assign servers to clusters as follows:

- **Spaces_Cluster:**
 - WC_Spaces1
 - WC_Spaces2
- **Portlet_Cluster:**
 - WC_Portlet1
 - WC_Portlet2
- **Collab_Cluster:**
 - WC_Collaboration1
 - WC_Collaboration2
- **Utilities_Cluster:**
 - WC_Uilities1
 - WC_Uilities2

Click **Next**.

16. In the Configure Machines screen, click the **Unix Machine** tab and ensure that the following four entries exist:

Table 10-5 Machines

Name	Node Manager Listen Address
SOAHOST1	SOAHOST1 SOAHOST1 was configured when you ran the Configuration Wizard in Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain."
SOAHOST2	SOAHOST2 SOAHOST2 was configured when you ran the Configuration Wizard in Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain."
WCPHOST1	WCPHOST1
WCPHOST2	WCPHOST2

Leave all other fields to their default values.

Click **Next**.

17. In the Assign Servers to Machines screen, assign servers to machines as follows:

- **ADMINHOST:**
 - AdminServer
- **SOAHOST1:**
 - WLS_WSM1
- **SOAHOST2:**
 - WLS_WSM2
- **WCPHOST1:**
 - WC_Spaces1
 - WC_Portlet1

- WC_Collaboration1
- WC_Uilities1
- **WCPHOST2:**
 - WC_Spaces2
 - WC_Portlet2
 - WC_Collaboration2
 - WC_Uilities2

Note: You can rename the originals servers, which appear by default in the Configuration Wizard, but do not delete them.

Click **Next**.

18. In the Target Deployment to Clusters or Servers screen, ensure the following targets:

- The **wsm-pm** application must be targeted only to **WSM-PM_Cluster**.
- The **oracle.wsm.seedpolicies** library must be targeted only to **WSM-PM_Cluster**.

Click **Next**.

19. In the Target Services to Clusters or Servers screen, ensure the following targets:

- Target **mds-owsm**, **mds-owsm-rac0**, and **mds-owsm-rac1** to both **WSM-PM_Cluster** and **AdminServer**.

Click **Next**.

20. In the Configuration Summary screen, do not change the values that appear on the screen (since you are extending a domain). Click **Extend**.

21. In the Extending Domain screen, click **Done**.

You must start the Administration Server for this configuration to take effect.

22. Start the Administration Server using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1"](#).

10.3 Post-Configuration Tasks

After extending the domain with the Configuration Wizard, follow these instructions for post-configuration.

This section includes the following topics:

- [Section 10.3.1, "Disabling Host Name Verification for the WebCenter Portal Managed Servers"](#)
- [Section 10.3.2, "Starting Node Manager on SOAHOST1"](#)
- [Section 10.3.3, "Propagating the Domain Changes to the Managed Server Domain Directory"](#)

10.3.1 Disabling Host Name Verification for the WebCenter Portal Managed Servers

In this guide, you set up the appropriate certificates to authenticate the different nodes with the Administration Server after you have completed the procedures to extend the domain for WebCenter Portal. Therefore, you must disable host name verification for the WebCenter Portal managed servers to avoid errors when managing the different WebLogic Servers. You enable host name verification again once the Enterprise Deployment topology configuration is complete. See [Section 11.5, "Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2"](#) for more information.

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Select **Servers**. The Summary of Servers page appears.
5. Select **WC_Spaces1** (represented as a hyperlink) from the Names column of the table. The Settings page appears.
6. Select the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set Hostname Verification to **None**.
9. Repeat these steps for the WC_Spaces2, WC_Portlet1, WC_Portlet2, WC_Collaboration1, WC_Collaboration2, WC_Uilities1, and WC_Uilities2 managed servers.
10. Save and activate the changes.
11. This change requires a restart of the Administration Server and Node Managers.
 - a. To restart the Administration Server see [Chapter 8.4.3, "Starting the Administration Server on SOAHOST1."](#)
 - b. To restart Node Manager on SOAHOST1, see [Chapter 10.3.2, "Starting Node Manager on SOAHOST1."](#)

10.3.2 Starting Node Manager on SOAHOST1

Use the `startNodeManager.sh` script to restart Node Manager.

To restart the Node Manager on SOAHOST1:

1. Stop Node Manager by stopping the process associated with it:
 - If it is running in the foreground in a shell, simply use **CTRL+C**.
 - If it is running in the background in the shell, find the associate process and use the `kill` command to stop it. For example:

```
ps -ef | grep NodeManager
orcl      9139  9120  0 Mar03 pts/6    00:00:00 /bin/sh
./startNodeManager.sh
```

```
kill -9 9139
```

2. Start Node Manager:

```
cd WL_HOME/server/bin
```



```
./startNodeManager.sh
```

10.3.3 Propagating the Domain Changes to the Managed Server Domain Directory

Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directory.

To propagate start scripts and classpath configuration:

1. Create a copy of the managed server domain directory and the managed server applications directory.
2. Run the `pack` command on SOAHOST1 to create a template pack using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name
-template=wcdomaintemplate.jar -template_name=wcdomaintemplate
```

3. Run the `unpack` command on SOAHOST1 to unpack the propagated template to the domain directory of the managed server using the following command:

```
./unpack.sh
-domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=wcdomaintemplate.jar
-overwrite_domain=true
-app_dir=ORACLE_BASE/admin/domain_name/mserver/apps
```

Note: The `-overwrite_domain` option in the `unpack` command, allows unpacking a managed server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the managed server domain directory, they must be re-applied after this unpack operation.

10.4 Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2

After completing the configuration of SOAHOST1, propagate the configuration to SOAHOST2, WCPHOST1, and WCPHOST2 using the `unpack` utility, and then validate the propagated configuration.

This section includes the following topics:

- [Section 10.4.1, "Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2 Using the `unpack` Utility"](#)
- [Section 10.4.2, "Starting the Node Manager on WCPHOST1 and WCPHOST2"](#)
- [Section 10.4.3, "Starting the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers on WCPHOST1"](#)
- [Section 10.4.4, "Validating the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers"](#)
- [Section 10.4.5, "Starting the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 Managed Servers on WCPHOST2"](#)

- [Section 10.4.6, "Validating the WC_Spaces2, WC_Portlet2, WC_Uutilities2, and WC_Collaboration2 Managed Servers"](#)

10.4.1 Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2 Using the unpack Utility

Propagate the domain you just configured to SOAHOST2, WCPHOST1, and WCPHOST2 using the unpack utility.

Note: If the Middleware homes are shared between systems, the domain template should already be in the proper directory and you can skip step 1 below.

To propagate the domain configuration:

1. Run the following commands on SOAHOST1 to copy the template file created earlier to SOAHOST2, WCPHOST1, and WCPHOST:

```
scp wcdomaintemplate.jar oracle@SOAHOST2:ORACLE_COMMON_HOME/common/bin
```

```
scp wcdomaintemplate.jar oracle@WCPHOST1:ORACLE_COMMON_HOME/common/bin
```

```
scp wcdomaintemplate.jar oracle@WCPHOST2:ORACLE_COMMON_HOME/common/bin
```

2. Run the unpack command on SOAHOST2, WCPHOST1, and WCPHOST2 to unpack the propagated template.

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./unpack.sh
```

```
-domain=ORACLE_BASE/admin/domain_name/mserver/domain_name/
```

```
-template=wcdomaintemplate.jar
```

```
-overwrite_domain=true
```

```
-app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

3. Repeat the above steps for WCPHOST1 and WCPHOST2.

10.4.2 Starting the Node Manager on WCPHOST1 and WCPHOST2

Use the `startNodeManager.sh` script to start Node Manager.

To start the Node Manager on WCPHOST1 and WCPHOST2:

1. Run the `setNMProps.sh` script, located in the `ORACLE_COMMON_HOME/common/bin` directory, to set the `StartScriptEnabled` property to 'true' before starting Node Manager on both WCPHOST1 and WCPHOST2:

```
WCPHOSTn> cd ORACLE_COMMON_HOME/common/bin
```

```
WCPHOSTn> ./setNMProps.sh
```

Note: You can skip step 1 if the WebCenter Portal server is sharing the Middleware home in a local or shared storage with SOA (as suggested in [Chapter 3, "Preparing the Network for an Enterprise Deployment"](#)), and SOA was configured earlier. In this instance, you do not need to `setNMPProps.sh` again, and Node Manager is already running on SOAHOST1 and SOAHOST2.

2. Run the following commands on both WCPHOST1 and WCPHOST2 to start Node Manager:

```
WCPHOST1> cd WL_HOME/server/bin
WCPHOST1> ./startNodeManager.sh
```

```
WCPHOST2> cd WL_HOME/server/bin
WCPHOST2> ./startNodeManager.sh
```

10.4.3 Starting the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers on WCPHOST1

To start the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 managed servers managed servers using the Administration Console:

1. Access the Administration Console at `http://ADMINVHN:7001/console`.
ADMINVHN is the virtual host name that maps to the virtual IP where the Administration Server is listening (in SOAHOST1).
2. Expand the **Environment** node in the **Domain Structure** window.
3. Click **Servers**.
4. Open the **Control** tab.
5. Select **WC_Spaces1**, **WC_Portlet1**, **WC_Uilities1**, and **WC_Collaboration1**.
6. Click **Start**.

10.4.4 Validating the WC_Spaces1, WC_Portlet1, WC_Uilities1, and WC_Collaboration1 Managed Servers

To validate that all the WebCenter Portal managed servers on WCPHOST1 are up and running:

1. Check that the managed servers are accessible by testing the following URLs:
 - `http://WCPHOST1:9000/webcenter`
 - `http://WCPHOST1:9000/webcenterhelp`
 - `http://WCPHOST1:9000/rss`
 - `http://WCPHOST1:9000/rest`
 - `http://WCPHOST1:9001/pagelets`
 - `http://WCPHOST1:9001/portalTools`
 - `http://WCPHOST1:9001/wsrp-tools`
 - `http://WCPHOST1:9002/owc_discussions`
 - `http://WCPHOST1:9003/activitygraph-engines/Login.jsp`

- `http://WCPHOST1:9003/wcps/api/property/resourceIndex`
2. Check that all deployments are active. In the Administration Console, select **Deployments**.
If any failed, check the log files for any errors. The log files can be found at `.ORACLE_BASE/admin/domain_name/mserver/domain_home/servers/server_name/logs`

10.4.5 Starting the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 Managed Servers on WCPHOST2

To start the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 managed servers managed servers using the Administration Console:

1. Access the Administration Console at `http://ADMINVHN:7001/console`.
ADMINVHN is the virtual host name that maps to the virtual IP where the Administration Server is listening (in SOAHOST1).
2. Expand the **Environment** node in the **Domain Structure** window.
3. Click **Servers**.
4. Open the **Control** tab.
5. Select **WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2**.
6. Click **Start**.

10.4.6 Validating the WC_Spaces2, WC_Portlet2, WC_Uilities2, and WC_Collaboration2 Managed Servers

To validate that all the WebCenter Portal managed servers on WCPHOST2 are up and running:

1. Check that the managed servers are accessible by testing the following URLs:
 - `http://WCPHOST2:9000/webcenter`
 - `http://WCPHOST2:9000/webcenterhelp`
 - `http://WCPHOST2:9000/rss`
 - `http://WCPHOST2:9000/rest`
 - `http://WCPHOST2:9001/pagelets`
 - `http://WCPHOST2:9001/portalTools`
 - `http://WCPHOST2:9001/wsrp-tools`
 - `http://WCPHOST2:9002/owc_discussions`
 - `http://WCPHOST2:9003/wcps/api/property/resourceIndex`
2. Check that all deployments are active. In the Administration Console, select **Deployments**.

If any failed, check the log files for any errors. The log files can be found at:

`.ORACLE_BASE/admin/domain_name/mserver/domain_home/servers/server_name/logs`

10.5 Configuring the Java Object Cache for Spaces_Cluster

Configure the Java Object Cache (JOC) among all the managed servers in Spaces_Cluster. This local cache is provided to increase the performance of the Spaces application.

The Java Object Cache can be configured using the `MW_HOME/oracle_common/bin/configure-joc.py` script. This is a Python script which can be used to configure JOC in the managed servers. The script runs in WLST online mode and expects the Administration Server to be up and running. For general information about WLST online mode, see "Getting Started Using the Oracle WebLogic Scripting Tool (WLST)" in *Oracle Application Server Administrator's Guide*.

Note: After configuring the Java Object Cache, using the WLST commands or `configure-joc.py` script, restart all affected managed servers for the configurations to take effect.

To configure the Java Object Cache for WebCenter Portal managed servers:

1. Connect to the Administration Server using WLST, for example:

```
MW_HOME/wc/common/bin/wlst.sh
$ connect()
```

Enter the Oracle WebLogic Administration user name and password when prompted.

2. After connecting to the Administration Server using WLST, start the script using the `execfile` command, for example:

```
wls:/mydomain/serverConfig>execfile("MW_HOME/oracle_
common/bin/configure-joc.py")
```

3. Configure JOC for all the managed servers for a given cluster.

Enter 'y' when the script prompts whether you want to specify a cluster name, and also specify the cluster name and discover port, when prompted. This discovers all the managed servers for the given cluster and configures the JOC. The discover port is common for the entire JOC configuration across the cluster.

Note: You can specify any free port for the "Discover Port".

Here is a walkthrough for using `configure-joc.py` for high availability environments:

```
execfile("MW_HOME/oracle_common/bin/configure-joc.py")
.
Enter Hostnames (eg host1,host2) : WCPHOST1,WCPHOST2
.
Do you want to specify a cluster name (y/n) <y>y
.
Enter Cluster Name : Spaces_Cluster
.
Enter Discover Port : 9988
.
Enter Distribute Mode (true|false) <true> : true
.
Do you want to exclude any server(s) from JOC configuration (y/n) <n> n
```

The script can also be used to perform the following JOC configurations:

- Configure JOC for all specified managed servers.

Enter 'n' when the script prompts whether you want to specify a cluster name, and also specify the managed server and discover port, when prompted. For example:

```
Do you want to specify a cluster name (y/n) <y>n
Enter Managed Server and Discover Port (eg WC_Spaces1:9988,WC_Spaces2:9988) :
WC_Spaces1:9988,WC_Spaces2:9988
```

- Exclude JOC configuration for some managed servers.

The script allows you to specify the list of managed servers for which the JOC configuration "DistributeMode" will be set to 'false'. Enter 'y' when the script prompts whether you want to exclude any servers from JOC configuration, and enter the managed server names to be excluded, when prompted. For example:

```
Do you want to exclude any server(s) from JOC configuration (y/n) <n>y
Exclude Managed Server List (eg Server1,Server2) : WC_Spaces1,WC_Spaces2
```

- Disable the distribution mode for all managed servers.

The script allows you to disable the distribution to all the managed servers for a specified cluster. Specify 'false' when the script prompts for the distribution mode. By default, the distribution mode is set to 'true'.

Verify JOC configuration using the CacheWatcher utility. See *Oracle Fusion Middleware High Availability Guide*.

You can configure the Java Object Cache (JOC) using the **HA Power Tools** tab in the Oracle WebLogic Administration Console as described in the *Oracle Fusion Middleware High Availability Guide*.

10.6 Converting Discussions from Multicast to Unicast

To convert Discussions (on all managed servers in the Collab_Cluster) from multicast to unicast, add the relevant startup parameters:

1. In the Oracle WebLogic Server Administration Console, select **Servers, WC_Collaboration1, Configuration**, and then **Server Start**.
2. In the Arguments box, add the following:

```
-Dtangosol.coherence.wka1=WCPHOST1
-Dtangosol.coherence.wka2=WCPHOST2
-Dtangosol.coherence.localhost=WCPHOST1
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
-Dtangosol.coherence.localport=8089
```

Where **WCPHOST1** is the host on which **WC_Collaboration1** is running.

Port 8089 is a port reserved for WebCenter Coherence communications.

3. Repeat steps 1 and 2 for **WC_Collaboration2**, swapping **WCPHOST1** for **WCPHOST2** and **WCPHOST2** for **WCPHOST1**.

```
-Dtangosol.coherence.wka1=WCPHOST2
-Dtangosol.coherence.wka2=WCPHOST1
-Dtangosol.coherence.localhost=WCPHOST2
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

-Dtangosol.coherence.localport=8089

- Restart the WC_Collaboration servers.

10.7 Configuring Clustering on the Discussions Server

If this is a unicast cluster, first complete all the steps in [Section 10.6, "Converting Discussions from Multicast to Unicast"](#).

To ensure that all members in the Discussions cluster can communicate with each other:

- Log in to the discussions server's Administration Console for each member of the cluster at:

`http://host:port/owc_discussions/admin`

- Select **Cache Settings**.

Figure 10–1 Cache Settings Section

Feature	Status	Description
Short-term Query Cache	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled: object lifetime: <input checked="" type="radio"/> 5 seconds <input type="radio"/> 10 seconds	Prevents cache expirations of the query cache from happening more than once every 5 or 10 seconds. This is useful for sites with extreme amounts of traffic. The ramification to using the short-term query cache is that new content wont appear for 5 to 10 seconds after its posted.
Clustering	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	You can enable or disable clustered caching in the system. Note: enabling clustering may take up to 30 seconds.

Save Settings Cancel

Discussions Server Administration Console

- In the **Cache Features** section, ensure that **Clustering** is set to **Enabled**.
As servers join the cluster they appear at the top of the screen.
- In the **Tool** section, select **Reset All Cluster Members** and the **Start Cache WarmUp Task**. Repeat the Cache warm up task on all members of the cluster.

Figure 10–2 Cache Tools Section

Tool	Description
Cache Warmup Task	<input type="button" value="Start Cache Warmup Task"/> The cache warmup process will load your caches with the data that is most likely to accessed by users. This action is useful to perform when first starting a server, or after flushing the cache. However, it will put a heavy load on your database for a few minutes.
Cluster-wide Cache Reset	<input type="button" value="Reset All Cluster Members"/> Clears all caches on all cluster members. This provides the easiest way to ensure that all clusters members are synchronized together properly. It is also a good way to recover if a server joins the cluster but is pointing to a database that the other cluster members are not using, resulting in corrupted caches.
Java Memory Monitor	<input type="checkbox"/> 95.90 MB of 997.75 MB(9.6%) used

Discussions Server Administration Console

- Repeat steps 1 through 4 for all members of the cluster.

As servers join the cluster they appear at the top of the screen.

10.8 Configuring Analytics

Out-of-the box, Analytics Collectors are configured to communicate with the local Spaces application in a 1-1 relationship (the collectors listen on localhost). No additional Analytics Collector configuration is required.

However, you must configure the Spaces applications to send event messages to localhost:

Note: Clustered Analytics Collectors are not supported for collecting WebCenter Portal events.

To connect the Spaces application to the analytics collector:

1. Connect to the managed server where the Spaces application is running using WLST, for example:

```
MW_HOME/wc/common/bin/wlst.sh
connect("weblogic_admin_username", "weblogic_admin_pwd", "WCPHOST1:9000")
```

Connect to the host and port of the WC_Spaces server.

2. Create a connection between the Spaces application and the Analytics Collector and make it the default connection (`default=1`).

For example:

```
createAnalyticsCollectorConnection(appName="webcenter", name="HAConn1",
isUnicast=1,
collectorHost="localhost", collectorPort=31314, isEnabled=1, timeout=30,
default=1)
```

See also, "createAnalyticsCollectorConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

3. Verify the changes made:

```
listDefaultAnalyticsCollectorConnection(appName="webcenter")
```

See also, "listDefaultAnalyticsCollectorConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

10.9 Configuring Activity Graph

Activity Graph should run as a singleton. In a cluster environment, all Activity Graph application instances should be disabled except for one.

To disable Activity Graph Engines applications:

1. Log in to the Administration Console.
2. Shut down the WC_Uilities1 and WC_Uilities2 servers.
3. Select **Deployments**
4. Click **Lock & Edit**.
5. Alter the targets for each of these deployments:
 - activitygraph-engines (11.1.1.6.0)

- oracle.webcenter.activitygraph.engine.lib (11.1.1,11.1.1)
 - oracle.webcenter.activitygraph.lib (11.1.1,11.1.1)
 - a. Select the deployment.
 - b. Select the **Targets** tab.
 - c. Click **Change Targets**.
 - d. Ensure that the deployment is only targeted to **Part of the Cluster/one of the Managed Servers** for Utilities_Cluster. Targeting to other servers and Clusters should remain unchanged.
 - e. Click **OK** to save the changes.
6. When finished with all three deployments, click **Activate all Changes**.
 7. Start up WC_Uilities1 and WC_Uilities2 servers.

Since Activity Graph is only running on one node, if this node is lost, or the Managed Server is not available, Activity Graph will be unavailable. In the case of node failure, Activity Graph can be manually deployed on any other available Managed Server in the cluster.

Note: Oracle does not recommend that you configure Server Migration for Activity Graph, since Activity Graph resides in the same server as other components that must not be failed over. For more information about server migration, see [Chapter 14, "Configuring Server Migration for an Enterprise Deployment"](#).

10.10 Configuring REST APIs

If you want to use WebCenter Portal REST APIs, you must perform the server-side configuration described in this section.

To seed entries in the credential store that enable the REST security tokens to function properly:

1. Connect to the Administration Server using the command-line Oracle WebLogic Scripting Tool (WLST), for example:

```
MW_HOME/wc/common/bin/wlst.sh
```

2. Run the following WLST commands to configure the credential store:

```
createCred(map="o.webcenter.jf.csf.map", key="keygen.algorithm",
           user="keygen.algorithm", password="AES")
createCred(map="o.webcenter.jf.csf.map", key="cipher.transformation",
           user="cipher.transformation", password="AES/CBC/PKCS5Padding")
```

Later on, you must configure REST policies in OAM ([Chapter 15.5.3.3, "Updating the REST Policies"](#)).

For more information on REST APIs, see the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

10.11 Configuring Oracle HTTP Server with the Extended Domain

This section includes the following topics:

- [Section 10.11.1, "Configuring Oracle HTTP Server for the WC_Spacesn, WC_Portletn, WC_Uilitiesn, and WC_Collaborationn Managed Servers"](#)
- [Section 10.11.2, "Validating Access Through Oracle HTTP Server"](#)
- [Section 10.11.3, "Validating Access Through the Load Balancer"](#)

10.11.1 Configuring Oracle HTTP Server for the WC_Spacesn, WC_Portletn, WC_Uilitiesn, and WC_Collaborationn Managed Servers

To enable Oracle HTTP Server to route to the WebCenter Portal clusters, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster. Add the following lines to the `OHS_HOME/instances/ohs_instance1/config/OHS/ohs1/mod_wl_ohs.conf` file on all WEBHOST machines. Keep any previous configuration for the Admin and SOA Servers. Restart all HTTP Servers when finished.

```
# Virtual Host for wcp.mycompany.com holds all the external URLs. The Virtual Host
should already exist
# and any existing Location blocks should be kept.
```

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

# Spaces Application
<Location /webcenter>
    WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /webcenterhelp>
    WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /rss>
    WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /rest>
    WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Discussions
<Location /owc_discussions>
    WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
    SetHandler weblogic-handler
```

```

        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>

# Portlets

    <Location /pagelets>
        WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>

    <Location /portalTools>
        WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>

    <Location /wsrp-tools>
        WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>

# Personalization

    <Location /wcps>
        WebLogicCluster WCPHOST1:9003,WCPHOST2:9003
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>

#Activity Graph
#The WebLogicHost below should be set to the Host on which ActivityGraph is
running.

    <Location /activitygraph-engines>
        WebLogicHost WCPHOST1
        WebLogicPort 9003
        WLProxySSL ON
        WLProxySSLPassThrough ON
    </Location>
</VirtualHost>

# Virtual host entry for internal http URL.
# This should already be in the config file. The new Location blocks go inside of
it

NameVirtualHost *:7777

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

```

```

# Portlet Internal access

<Location /pagelets>
  WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
  SetHandler weblogic-handler
</Location>

<Location /portalTools>
  WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
  SetHandler weblogic-handler
</Location>

<Location /wsrp-tools>
  WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
  SetHandler weblogic-handler
</Location>

# Discussions Internal access
<Location /owc_discussions>
  WebLogicCluster WCPHOST1:9001,WCPHOST2:9002
  SetHandler weblogic-handler
</Location>

</VirtualHost>

#Virtual host for SharePoint access
<VirtualHost *:7777>
  ServerName wcp-spaces.mycompany.com
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit

#SharePoint entry point
<Location />
  WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

# Spaces Application
<Location /webcenter>
  Deny from all
</Location>

<Location /webcenterhelp>
  Deny from all
</Location>

<Location /rss>
  Deny from all
</Location>

<Location /rest>
  Deny from all
</Location>

</VirtualHost>

```

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

Some example scenarios:

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

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

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

10.11.1.1 Configuring Microsoft Clients

In order to accommodate Microsoft Clients, refer to the overview and detailed steps outlined in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

In particular, you must create another Virtual Host in order to provide a separate context root for these clients. For instructions see "Configuring SSO with Virtual Hosts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

Follow the steps in "Configuring SSO for Microsoft Clients" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal* to properly configure Windows authentication services.

10.11.2 Validating Access Through Oracle HTTP Server

Verify that you can access these URLs:

- `http://WEBHOSTn:7777/webcenter`
- `http://WEBHOSTn:7777/webcenterhelp`
- `http://WEBHOSTn:7777/rss`
- `http://WEBHOSTn:7777/rest`
- `http://WEBHOSTn:7777/pagelets`
- `http://WEBHOSTn:7777/portalTools`
- `http://WEBHOSTn:7777/wsrp-tools`
- `http://WEBHOSTn:7777/owc_discussions`
- `http://WEBHOSTn:7777/activitygraph-engines/Login.jsp`
- `http://WEBHOSTn:7777/wcps/api/property/resourceIndex`

Where `WEBHOSTn` specifies the name of each Oracle HTTP Server host (for example, `WEBHOST1`, `WEBHOST2`).

10.11.3 Validating Access Through the Load Balancer

Verify that you can access these URLs:

- `https://wcp.mycompany.com/webcenter`
- `https://wcp.mycompany.com/webcenterhelp`
- `https://wcp.mycompany.com/rss`
- `https://wcp.mycompany.com/rest`
- `https://wcp.mycompany.com/pagelets`
- `https://wcp.mycompany.com/portalTools`
- `https://wcp.mycompany.com/wsrp-tools`
- `https://wcp.mycompany.com/owc_discussions`
- `https://wcp.mycompany.com/activitygraph-engines/Login.jsp`
- `https://wcp.mycompany.com/wcps/api/property/resourceIndex`

10.12 Backing Up the WebCenter Portal Configuration

After you have verified that the extended domain is working, back up the domain configuration. This is a quick backup for the express purpose of immediate restore in case of failures in future procedures. Back up the configuration to the local disk. This backup can be discarded once you have completed the enterprise deployment. Once you have completed the enterprise deployment, you can initiate the regular deployment-specific backup and recovery process.

For information about backing up the environment, see "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*. For information about recovering your information, see "Recovering Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

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 this guide. For information on how to recover components, see "Recovery of Components" and "Recovery After Loss of Component" sections in the 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 domain configuration:

1. Back up the web tier:

- a. Shut down the instance using `opmnctl`.

```
ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
```

- 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 using `opmnctl`:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl startall
```

2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or OS tools such as `tar` for cold backups if possible.
3. Back up the AdminServer domain directory. Perform a backup to save your domain configuration. The configuration files are located in the following directory:

```
ORACLE_BASE/admin/domain_name
```

To back up the Administration Server run the following command on SOHOST1:

```
tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Setting Up Node Manager for an Enterprise Deployment

This chapter describes how to configure Node Manager according to the Enterprise Deployment recommendations.

This chapter includes the following sections:

- [Section 11.1, "Overview of the Node Manager"](#)
- [Section 11.2, "Changing the Location of Node Manager Log"](#)
- [Section 11.3, "Enabling Host Name Verification Certificates for Node Manager in SOAHOST1 and WCPHOST1"](#)
- [Section 11.4, "Starting the Node Manager on SOAHOST1"](#)
- [Section 11.5, "Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2"](#)
- [Section 11.6, "Starting Node Manager on SOAHOST2"](#)
- [Section 11.7, "Configuring WebLogic Servers to Use the Custom Keystores"](#)

11.1 Overview of the Node Manager

The Node Manager enables you to start and stop the Administration Server and the managed servers.

Oracle recommends using host name verification for the communications between Node Manager and the Administration Server. This requires the use of certificates for the different addresses communicating with the Administration Server. In this chapter, the steps for configuring SOAHOST1 and SOAHOST2 certificates for host name verification are provided. Similar steps are required for WCPHOST1 and WCPHOST2. Although the appropriate host name changes in the steps are required for WCPHOST1 and WCPHOST2, the procedure and syntax are exactly the same.

11.2 Changing the Location of Node Manager Log

Oracle recommends placing your Oracle Fusion Middleware deployment's Node Manager's log in a different location from the default (which is inside the MW_Home where Node Manager is located).

To change the location of the Node Manager log, edit the `nodemanager.properties` file located in the following directory:

```
MW_HOME/wlserver_10.3/common/nodemanager
```

Oracle recommends locating this file outside of the *MW_HOME* directory, and inside the admin directory for the deployment.

Add the following line to `nodemanager.properties`:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Restart Node Manager for the change to take effect.

11.3 Enabling Host Name Verification Certificates for Node Manager in SOAHOST1 and WCPHOST1

Host name verification enables communication between Node Manager and the Administration Server. This verification requires the use of certificates for the different addresses communicating with the Administration Server.

This section contains the following topics:

- 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: [Using a Common or Shared Storage Installation](#)

11.3.1 Generating Self-Signed Certificates Using the `utils.CertGen` Utility

This section describes the procedure for creating self-signed certificates on `SOAHOST1.mycompany.com`. Create these certificates using the network name/alias.

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 (for example, SSL set up for HTTP invocations). In this case, `SOAHOST2`, `WCPHOST1` and `WCPHOST2` uses the `cert` directory created for `SOAHOST1` certificates.

For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

About Passwords

The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that include both uppercase and lowercase characters as well as numbers.

To create self-signed certificates:

1. Set up your environment by running the `WL_HOME/server/bin/setWLSEnv.sh` script:

In the Bourne shell, run the following command on `SOAHOST1`:

```
. setWLSEnv.sh
```

Verify that the `CLASSPATH` environment variable is set:

```
echo $CLASSPATH
```

2. Create a user-defined directory for the certificates.

```
mkdir certs
```

3. Change directory to the user-defined directory.

```
cd certs
```

4. Run the `utils.CertGen` tool from the user-defined directory to create the certificates SOAHOST1, SOAHOST1VHN VIP, the Admin VIP, and WCPHOST1.

Syntax:

```
java utils.CertGen key_passphrase cert_file_name key_file_name [export | domestic] [hostname]
```

Example commands from SOAHOST1:

```
java utils.CertGen welcome1 SOAHOST1.mycompany.com_cert SOAHOST1.mycompany.com_key domestic SOAHOST1.mycompany.com
```

```
java utils.CertGen welcome1 SOAHOST1VHN1.mycompany.com_cert SOAHOST1VHN1.mycompany.com_key domestic SOAHOST1VHN1.mycompany.com
```

```
java utils.CertGen welcome1 ADMINVHN.mycompany.com_cert ADMINVHN.mycompany.com_key domestic ADMINVHN.mycompany.com
```

```
java utils.CertGen welcome1 WCPHOST1.mycompany.com_cert WCPHOST1.mycompany.com_key domestic WCPHOST1.mycompany.com
```

11.3.2 Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility

The procedures described in the previous sections created an identity keystore that resides in a shared storage. In this section, new keys for SOAHOST1 and WCPHOST1 are added to the store. Import the certificate and private key for SOAHOST1, SOAHOST1VHN1, ADMINVHN and WCPHOST1 into the Identity Store. Make sure you use a different alias for each of the certificate/key pairs imported.

Follow these steps to create an identity keystore on SOAHOST1:

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/cert`).

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 SOAHOST1, SOAHOST1VHN VIP, the Admin VIP, and WCPHOST 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:

```
java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity1 welcome1
ORACLE_BASE/admin/domain_name/cert/SOAHOST1.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/SOAHOST1.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity2 welcome1
ORACLE_BASE/admin/domain_name/cert/SOAHOST1VHN1.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/SOAHOST1VHN1.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity3 welcome1
ORACLE_BASE/admin/domain_name/cert/ADMINVHN.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/ADMINVHN.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity4 welcome1
ORACLE_BASE/admin/domain_name/cert/WCPHOST1.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/WCPHOST1.mycompany.com_key.pem
```

11.3.3 Creating a Trust Keystore Using the Keytool Utility

To create the Trust Keystore on SOAHOST1.mycompany.com.

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 key store directly. Copy the standard Java keystore CA certificates located under the *WL_HOME/server/lib* directory to the same directory as the certificates. For example:

```
cp WL_HOME/server/lib/cacerts
ORACLE_BASE/admin/domain_name/asever/domain_namecerts/appTrustKeyStore.jks
```

2. The default password for the standard Java keystore is *changeit*. Oracle recommends always changing the default password. Use the keytool utility on *HOST* to do this. The syntax is:

```
keytool -storepasswd -new NewPassword -keystore TrustKeyStore -storepass
Original_Password
```

For example:

```
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 and is located at *WL_HOME/server/lib* directory. This CA certificate must be imported into the *appTrustKeyStore* using the keytool utility on *HOST*. The syntax is:

```
keytool -import -v -noprompt -trustcacerts -alias AliasName
-file CAFileLocation -keystore KeyStoreLocation -storepass KeyStore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file
WL_HOME/server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass
welcome1
```

11.3.4 Configuring Node Manager to Use the Custom Keystores

To configure the 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 Passwd
CustomIdentityAlias=Identity Key Store 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 on **SOAHOST1**, use **appIdentity1** according to the steps in [Section 11.3.3, "Creating a Trust Keystore Using the Keytool Utility"](#):

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity1
CustomIdentityPrivateKeyPassPhrase=welcome1
```

The passphrase entries in the `nodemanager.properties` file are encrypted when you start Node Manager as described in [Section 11.4, "Starting the Node Manager on SOAHOST1."](#) For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, start Node Manager as soon as possible so that the entries are encrypted.

11.3.5 Using a Common or Shared Storage Installation

When using a common or shared storage installation for `MW_HOME`, Node Manager is started from different nodes using the same base configuration (`nodemanager.properties`). Add the certificate for all the nodes that share the binaries to the `appIdentityKeyStore.jks` identity store by creating the certificate for the new node and import it to `appIdentityKeyStore.jks` as described in [Section 11.3.1, "Generating Self-Signed Certificates Using the `utils.CertGen` Utility."](#) Once the certificates are available in the store, each node manager must point to a different identity alias to send the correct certificate to the Administration Server.

Some examples showing how to set different environment variables before starting Node Manager in the different nodes:

```
SOAHOST1> cd WL_HOME/server/bin
SOAHOST1> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentitySOAHOST1

SOAHOST2> cd WL_HOME/server/bin
SOAHOST2> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentitySOAHOST2

WCPHOST1> cd WL_HOME/server/bin
WCPHOST1> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityWCPHOST1

WCPHOST2> cd WL_HOME/server/bin
WCPHOST2> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityWCPHOST2
```

11.4 Starting the Node Manager on SOAHOST1

Start Node Manager on SOAHOST1 using the `startNodeManager.sh` script.

Note: If you have not configured and started Node Manager yet, run the `setNMProps.sh` script as specified in section [Section 8.4.2, "Starting Node Manager on SOAHOST1."](#) This enables the use of the start script which is required for SOA.

To start Node Manager on SOAHOST1:

```
cd WL_HOME/server/bin
export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX
./startNodeManager.sh
```

Note: Ensure that you specify the custom identity alias specifically assigned to each host, so `appIdentity1` for ...HOST1 and `appIdentity2` for ...HOST2, and so on.

11.5 Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2

Host name verification enables communication between Node Manager and the Administration Server. This verification requires the use of certificates for the different addresses communicating with the Administration Server.

Perform these steps to set up SSL for communication between the Node Manager and the Administration Server:

- Step 1: [Generating Self-Signed Certificates Using the `utils.CertGen` Utility](#)
- Step 2: [Creating an Identity Keystore in 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](#)

11.5.1 Generating Self-Signed Certificates Using the `utils.CertGen` Utility

This section describes the procedure for creating self-signed certificates on SOAHOST2 and WCPHOST2. Create these certificates using the network name/alias.

The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the Administration Server, SOA servers, or WCP servers fail over, (manually or with server migration), the nodes can access the appropriate certificates. In this case, SOAHOST2 uses the cert directory created for SOAHOST1 certificate and WCPHOST2 uses the cert directory created for WCPHOST1 certificates. If you are maintaining duplicated stores, create user-defined directory for the certificates.

Create self-signed certificates using the `utils.CertGen` utility using the network name/alias.

For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

To create self-signed certificates on SOAHOST2 and WCPHOST2:

1. Set up your environment by running the `WL_HOME/server/bin/setWLSEnv.sh` script:

In the Bourne shell, run the following command:

```
. setWLSEnv.sh
```

Verify that the CLASSPATH environment variable is set:

```
echo $CLASSPATH
```

2. Create a user-defined directory for the certificates.

```
mkdir certs
```

3. Change directory to the user-defined directory.

```
cd certs
```

4. Run the utils.CertGen tool from the user-defined directory to create the certificates for both SOAHOST2, SOAHOST2VHN1, and WCPHOST2.

Syntax:

```
java utils.CertGen key_passphrase cert_file_name key_file_name [export | domestic] [host_name]
```

Examples:

```
java utils.CertGen welcome1 SOAHOST2_cert SOAHOST2_key
                        domestic SOAHOST2.mycompany.com
```

```
java utils.CertGen welcome1 SOAHOST2VHN1_cert SOAHOST2VHN1_key
                        domestic SOAHOST2VHM1.mycompany.com
```

```
java utils.CertGen welcome1 WCPHOST2_cert WCPHOST2_key
                        domestic WCPHOST1.mycompany.com
```

11.5.2 Creating an Identity Keystore in Using the utils.ImportPrivateKey Utility

The procedures described in the previous sections created an Identity keystore that resides in a shared storage. In this section new keys for SOAHOST2 and WCPHOST2 are added to the store. Import the certificate and private key for SOAHOST2, SOAHOST2VHN1, and WCPHOST2 into the Identity Store. Make sure you use a different alias for each of the certificate/key pairs imported.

Follow these steps to create an identity keystore on SOAHOST2.mycompany.com:

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/cert*).

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 SOAHOST2, SOAHOST2VHN1, and WCPHOST2 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:

```
java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1  
appIdentity1 welcome1  
ORACLE_BASE/admin/domain_name/cert/SOAHOST2.mycompany.com_cert.pem  
ORACLE_BASE/admin/domain_name/cert/SOAHOST2.mycompany.com_key.pem  
  
java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1  
appIdentity2 welcome1  
ORACLE_BASE/admin/domain_name/cert/SOAHOST2VHN1.mycompany.com_cert.pem  
ORACLE_BASE/admin/domain_name/cert/SOAHOST2VHN1.mycompany.com_key.pem  
  
java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1  
appIdentity4 welcome1  
ORACLE_BASE/admin/domain_name/cert/WCPHOST2.mycompany.com_cert.pem  
ORACLE_BASE/admin/domain_name/cert/WCPHOST2.mycompany.com_key.pem
```

11.5.3 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores:

1. 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 Passwd  
CustomIdentityAlias=Identity Key Store Alias  
CustomIdentityPrivateKeyPassPhrase=Private Key used when creating Certificate
```

Make sure to use the correct value for `CustomIdentityAlias` on each node.

For example, on `SOAHOST2`, with "appIdentity3".

```
KeyStores=CustomIdentityAndCustomTrust  
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/asever/domain_  
name/certs/appIdentityKeyStore.jks  
CustomIdentityKeyStorePassPhrase=welcome1  
CustomIdentityAlias=appIdentity3  
CustomIdentityPrivateKeyPassPhrase=welcome1
```

Note: The passphrase entries in the `nodemanager.properties` file get encrypted when you start Node Manager, as described in [Section 11.6, "Starting Node Manager on SOAHOST2."](#)

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.

11.6 Starting Node Manager on SOAHOST2

Start Node Manager on SOAHOST2 using the `startNodeManager.sh` script.

Note: If you have not configured and started Node Manager yet, run the `setNMProps.sh` script as specified in section [Section 8.4.2, "Starting Node Manager on SOAHOST1."](#) This enables the use of the start script which is required for SOA.

To start Node Manager on SOAHOST2:

```
cd WL_HOME/server/bin
export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX
./startNodeManager.sh
```

Note: Ensure that you specify the custom identity alias specifically assigned to each host, so `appIdentity1` for ...HOST1 and `appIdentity2` for ...HOST2, and so on.

11.7 Configuring WebLogic Servers to Use the Custom Keystores

Configure the WebLogic Servers to use the custom keystores using the Oracle WebLogic Server Administration Console. Complete this procedure for the Administration Server, and all the managed servers (`WLS_WSMn`, `WLS_SOAn`, `WC_Spacesn`, `WC_Collaborationn`, `WC_Uilitiesn`, and `WC_Portletn`).

The example directory path given in Step 6 is just an example. Oracle does not recommend putting keystores into the `aserver` directory, but recommends putting the keystore in shared storage. Having a separate directory for certificates is a better solution.

To configure the identity and trust keystores:

1. Log in to the Administration Console, and click **Lock & Edit**.
2. In the left pane, expand **Environment**, and select **Servers**.
3. Click the name of the server for which you want to configure the identity and trust keystores.
4. Select **Configuration**, and then **Keystores**.
5. 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.
6. In the **Identity** section, define attributes for the identity keystore.
 - a. **Custom Identity Keystore:** Enter the fully qualified path to the identity keystore:


```
ORACLE_BASE/admin/domain_name/aserver/domain_
name/certs/appIdentityKeyStore.jks
```
 - b. **Custom Identity Keystore Type:** Leave this field blank, it defaults to JKS.
 - c. **Custom Identity Keystore Passphrase:** Enter the password `Keystore_Password` you provided in [Section 11.3.2, "Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility."](#)

This attribute may be 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 reads only from the keystore, so whether or not you define this property depends on the requirements of the keystore.

7. In the **Trust** section, define properties for the trust keystore:
 - a. **Custom Trust Keystore:** Enter the fully qualified path to the trust keystore:


```
ORACLE_BASE/admin/domain_name/aserver/domain_
name/certs/appTrustKeyStore.jks
```
 - b. **Custom Trust Keystore Type:** Leave this field blank, it defaults to JKS.
 - c. **Custom Trust Keystore Passphrase:** The password you provided in as *New Password* in [Section 11.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#)

As mentioned in the previous step, this attribute may be optional or required depending on the type of keystore.
8. Click **Save**.
9. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
10. Select **Configuration**, then **SSL**.
11. 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 11.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#)
12. Click **Save**.
13. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
14. Restart the server for which the changes have been applied.
15. Repeat these steps for the Administration Server, and all the managed servers (WLS_WSM n , WLS_SOAN, WC_Spaces n , WC_Collaboration n , WC_Uilities n , and WC_Portlet n).
16. Verify that the communication between Node Manager, Administration Server and the managed servers is correct by enabling hostname verification:
 1. For each server, in the Administration Console, select **Configuration**, **SSL**, **Advanced**, **Hostname Verification**, and then **BEA HostName Verifier**.
 2. Restart the servers using the Administration Console.

Configuring External WebCenter Portal Services for an Enterprise Deployment

This chapter describes how to configure external services for WebCenter Portal applications using Fusion Middleware Control or WLST commands. For most external services, you must set up a connection between the WebCenter Portal application and the backend server.

This chapter contains the following sections:

- [Section 12.1, "Configuring the Discussions Server Connection"](#)
- [Section 12.2, "Configuring the Instant Messaging and Presence \(IMP\) Server Connection"](#)
- [Section 12.3, "Configuring a BPEL Server Connection for Worklists and Workflows"](#)
- [Section 12.4, "Registering Portlet Producers"](#)
- [Section 12.5, "Registering the Pagelet Producer"](#)
- [Section 12.6, "Configuring Search Services"](#)
- [Section 12.7, "Configuring the Mail Server for Notifications"](#)

12.1 Configuring the Discussions Server Connection

If you want to provide Discussions or Announcement services in a WebCenter Portal application you must connect your application to a discussions server. To configure a connection for the WebCenter Portal Enterprise Deployment, the following values are required:

- Server URL: **http://wcpinternal.mycompany.com/owc_discussions**
- Admin User: **discussions server admin user name**
- Admin Password: **discussions server admin password**

You can connect to a discussions server using Fusion Middleware Control or WLST commands:

- [Section 12.1.2, "Creating a Discussions Server Connection using WLST"](#)
- [Section 12.1.1, "Creating a Discussions Server Connection Using Fusion Middleware Control"](#)

For more information, see "Managing the Announcements and Discussions Services" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

12.1.1 Creating a Discussions Server Connection Using Fusion Middleware Control

To connect your WebCenter Portal application to a discussions server using Fusion Middleware Control:

1. Ensure that at least one of the managed server on which your application is deployed is up and running.
For example, for the Spaces application, one of the WC_Spaces managed servers.
2. Log on to the Enterprise Manager Fusion Middleware Control Console at `http://SOAHOST1:7001/em`.
3. Navigate to the home page for your WebCenter Portal application.
For example, to navigate to the home page for the Spaces application, select **Farm_wcpedg_domain, WebCenter > Portal > Spaces**, and then **webcenter (WC_Spaces1)**.
4. From the WebCenter Portal drop-down menu, select **Settings**, and then **Service Configuration**.
5. Click **Discussions and Announcements**, and then **Add**.
6. In the Add Discussion and Announcement Connection screen:
 - **Connection Name:** DFConnection
 - **Active Connection:** Select check box to enable the connection
 - **Server URL:** `http://wcpinternal.mycompany.com/owc_discussions`
 - **Administrator User Name:** Name of a discussions server user with admin permissions
7. Click **OK** to save the settings.
8. Restart the managed servers on which the application is deployed.
For the Spaces application, restart all the managed servers in the Spaces_Cluster.

12.1.2 Creating a Discussions Server Connection using WLST

To connect your WebCenter Portal application to a discussions server using the WebLogic Scripting Tool:

1. Start the WebLogic Scripting Tool:

```
WCPHOST1> MW_HOME/wc/common/bin/wlst.sh
```
2. In WLST, connect as the administrator.
For example:

```
connect("weblogic","admin_password","ADMINVHN:7001")
```
3. Use the `createDiscussionForumConnection` command to connect to the discussions server.
For example:

```
createDiscussionForumConnection(appName="webcenter",name="DFConnection",url="http://wcpinternal.mycompany.com/owc_discussions",adminUser="myDS_admin",default=1,server="WC_Spaces1")
```


Where `webcenter` is the name of the Spaces application deployed on WC_Spaces1.

See also, "createDiscussionForumConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

4. Restart the managed servers on which the application is deployed.
For the Spaces application, restart all the managed servers in the Spaces_Cluster.

12.2 Configuring the Instant Messaging and Presence (IMP) Server Connection

For instructions how to configure Instant Messaging and Presence servers, see "Registering Instant Messaging and Presence Servers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*

12.3 Configuring a BPEL Server Connection for Worklists and Workflows

The Worklist service and workflows, such as Spaces membership workflows, require a connection to a BPEL server. To configure a connection for the WebCenter Portal Enterprise Deployment, the following value is required:

- SOAP Server URL: **http://wcpinternal.mycompany.com**

You can connect to a BPEL server using Fusion Middleware Control or WLST commands:

- [Section 12.3.1, "Before You Start"](#)
- [Section 12.3.2, "Configuring Worklists and Workflow using Fusion Middleware Control"](#)
- [Section 12.3.3, "Configuring Worklist and Workflow using WLST"](#)

12.3.1 Before You Start

Before you connect your WebCenter Portal application to the BPEL server that will host the Worklist and Workflow application:

1. Complete prerequisites steps for the Worklist service.
For details, see "Back-End Requirements for the Worklist Service" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.
2. (Spaces application only) Complete prerequisites steps for the Spaces workflows.
For details, see "Back-End Requirements for WebCenter Portal: Spaces Workflows" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

12.3.2 Configuring Worklists and Workflow using Fusion Middleware Control

To connect your WebCenter Portal application to a BPEL server using Fusion Middleware Control:

1. Ensure that at least one of the managed server on which your application is deployed is up and running.
For example, for the Spaces application, one of the WC_Spaces managed servers.
2. Log on to the Enterprise Manager Fusion Middleware Control Console at `http://SOAHOST1:7001/em`.
3. Navigate to the home page for your WebCenter Portal application.

For example, to navigate to the home page for the Spaces application, select **Farm_wcpedg_domain, WebCenter > Portal > Spaces**, and then **webcenter (WC_Spaces1)**.

4. Configure a Worklist connection:
 - a. From the WebCenter Portal drop-down menu, select **Settings**, and then **Service Configuration**.
 - b. Click **Worklist**, and then **Add**.
 - c. In the Add Worklist Connection screen:
 - Connection Name:** WorklistConnection
 - Active Connection:** Select check box to enable the connection for the Worklist service
 - BPEL SOAP URL:** http://wcpinternal.mycompany.com
 - d. Click **OK** to save the settings.
5. (Spaces application only) Specify the BPEL server that is hosting the Spaces workflows:
 - a. From the WebCenter Portal drop-down menu, select **Settings**, and then **Application Configuration**.
 - b. From the **Connection Name** dropdown, choose the BPEL server connection where the workflows are deployed.
 - If the BPEL server connection you want is not listed, follow step 4 to set up the connection.
 - c. Click **OK** to save the settings.
6. Restart the managed servers on which the application is deployed.
 - For the Spaces application, restart all the managed servers in the Spaces_Cluster.

12.3.3 Configuring Worklist and Workflow using WLST

To connect your WebCenter Portal application to a BPEL server, and specify a BPEL server for the Worklist service and Spaces workflows using WLST:

1. Start the WebLogic Scripting Tool:

```
WCPHOST1> MW_HOME/wc/common/bin/wlst.sh
```

2. In WLST, connect as the administrator.

For example:

```
connect("weblogic","admin password","ADMINVHN:7001")
```

3. Configure a BPEL server connection:

For example:

```
createBPELConnection(appName="webcenter", name="WorklistConnection",
url="http://wcpinternal.mycompany.com", server="WC_Spaces1")
```

Where `webcenter` is the name of the Spaces application deployed on `WC_Spaces1`.

See also, "createBPELConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

4. Configure the Worklist service to use the BPEL connection:

For example:

```
addWorklistConnection (appName="webcenter", name="WorklistConnection",
verbose=1, server="WC_Spaces1")
```

See also, "addWorklistConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. (Spaces application only) Specify the connection that points to the BPEL server on which Spaces workflows are deployed.

For example:

```
setSpacesWorkflowConnectionName (appName="webcenter",
name="WorklistConnection", server="WC_Spaces1")
```

```
getSpacesWorkflowConnectionName (appName="webcenter", server="WC_Spaces1")
```

See also, "setSpacesWorkflowConnectionName" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

6. Restart the managed servers on which the application is deployed.

For the Spaces application, restart all the managed servers in the Spaces_Cluster.

12.4 Registering Portlet Producers

Several out-of-the-box portlet producers can be registered with WebCenter Portal applications. In the WebCenter Portal Enterprise Deployment, the required producer URLs are as follows:

- WSRP Producer URL:
<http://wcpinternal.mycompany.com/wsrp-tools/portlets/wsrp2?WSDL>
- WebClipping Producer URL:
<http://wcpinternal.mycompany.com/portalTools/webClipping/providers>
- OmniPortlet Producer URL:
<http://wcpinternal.mycompany.com/portalTools/omniPortlet/providers>

You can register portlet producers using Fusion Middleware Control or WLST commands:

- [Section 12.4.1, "Registering Out-of-the-Box Portlet Producers using Fusion Middleware Control"](#)
- [Section 12.4.2, "Registering Out-of-the-Box Portlet Producers Using WLST"](#)

12.4.1 Registering Out-of-the-Box Portlet Producers using Fusion Middleware Control

For details on how to register portlet producers using Fusion Middleware Control, see "Managing Portlet Producers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

12.4.2 Registering Out-of-the-Box Portlet Producers Using WLST

To register out-of-the-box portlet producers using WLST:

1. Start the WebLogic Scripting Tool:

```
WCPHOST1> MW_HOME/wc/common/bin/wlst.sh
```

2. In WLST, connect as the administrator.

For example:

```
connect("weblogic", "admin password", "ADMINVHN:7001", server="WC_Spaces1")
```

3. Register all three out-of-the-box WSRP and PDK-Java producers.

For example:

```
registerOOTBProducers(producerHost='wcpinternal.mycompany.com', producerPort=80,  
appName='webcenter', server=WC_Spaces1')
```

Where `webcenter` is the name of the Spaces application deployed on `WC_Spaces1`.

See also, "registerOOTBProducers" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

12.5 Registering the Pagelet Producer

If you want to expose WSRP and Oracle JPDK portlets and OpenSocial gadgets as pagelets in WebCenter Portal applications, you must register the Pagelet Producer. In the WebCenter Portal Enterprise Deployment, the required Pagelet Producer URL is:

<http://wcpinternal.mycompany.com/pagelets>

You can register the Pagelet Producer using Fusion Middleware Control or WLST commands. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal* for detailed steps:

- Registering the Pagelet Producer for WebCenter Portal Applications Using Fusion Middleware Control
- Registering the Pagelet Producer for WebCenter Portal Applications Using WLST

12.6 Configuring Search Services

You can configure Oracle Secure Enterprise Search (Oracle SES) services and crawlers using procedures in "Managing Oracle SES Search in WebCenter Portal" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

Ensure that:

- Oracle Secure Enterprise Search is registered with Oracle Internet Directory and the WebCenter Portal application is configured as an Oracle SES trusted entity, as described in "Oracle SES - Configuration" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.
- Connection exists between the WebCenter Portal application and Oracle Secure Enterprise Search, as described "Setting Up Oracle SES Connections" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

Ensure that any new URLs are added for both WEBHOST Oracle HTTP Server configurations as follows:

```
<Location /rsscrawl>  
  WebLogicCluster WCPHOST1:9000,WCPHOST2:9000  
  SetHandler weblogic-handler  
</Location>
```

```
<Location /sesUserAuth>
```



```

WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
SetHandler weblogic-handler
</Location>

```

See also, [Section 10.11.1, "Configuring Oracle HTTP Server for the WC_Spacesn, WC_Portletn, WC_Utilitysn, and WC_Collaborationn Managed Servers"](#).

12.7 Configuring the Mail Server for Notifications

For details on how to set up the Notifications service for WebCenter Portal applications, refer to "Setting Up Notifications" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

In a WebCenter Portal Enterprise Deployment, if you choose to send notifications using mail you must set an additional property on the mail server connection named `mail.user.emailAddress` which overrides any *Sender Mail Address* that is configured for mail notifications (that is, the 'From' field). If you do not set this additional property, one of the server names in the cluster appends to the *Sender Mail Address*, for example `sender_mail_address@server1`.

You can set additional properties for mail server connections using Fusion Middleware Control or WLST. For details, see:

- Registering Mail Servers Using Fusion Middleware Control (Table 17-7)
- Registering Mail Servers Using WLST

For example, using WLST:

```

setMailConnectionProperty(appName='webcenter', name='myMail_
Server_Connection_Name', key='mail.user.emailAddress',
value='myShared_User_Email_Address')

```

Where:

`myMail_Server_Connection_Name` - Name of the mail server connection used by the Notification service.

`myShared_User_Email_Address` - The SHARED mail address. This is the mail address associated with the user specified in the external application's *shared credentials*. Ensure you can login with this mail address to your mail server.

Extending the Domain to Include Oracle WebCenter Content

This chapter describes how to extend and configure a domain with Oracle WebCenter Content, for use in a WebCenter Portal enterprise deployment.

This chapter contains the following sections:

- Section 13.1, "Overview of Extending the Domain to Include Oracle WebCenter Content"
- Section 13.2, "Extending the Domain to Include Oracle WebCenter Content"
- Section 13.3, "Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility"
- Section 13.4, "Configuring the Load Balancer to Route WebCenter Content Traffic"
- Section 13.5, "Starting Node Manager on WCPHOST1 and WCPHOST2"
- Section 13.6, "Restarting the Administration Server"
- Section 13.7, "Starting and Configuring the WLS_WCC1 Managed Server"
- Section 13.8, "Updating the cwallet File in the Administration Server"
- Section 13.9, "Starting and Configuring the WLS_WCC2 Managed Server"
- Section 13.10, "Configuring Service Retries for Oracle WebCenter Content"
- Section 13.11, "Configuring Oracle HTTP Server for the WLS_WCC Managed Servers"
- Section 13.12, "Validating Access Through Oracle HTTP Server"
- Section 13.13, "Backing Up the Installation"
- Section 13.14, "Configure Oracle WebCenter Content for Oracle WebCenter Portal"
- Section 13.15, "Registering Oracle WebCenter Content with Oracle WebCenter Portal Applications"
- Section 13.16, "Installing and Configuring the Inbound Refinery"

Note: Before starting the setup process, read the *Oracle Fusion Middleware Release Notes* for additional installation and deployment information.

13.1 Overview of Extending the Domain to Include Oracle WebCenter Content

The Oracle WebCenter Content system is installed using the WL_HOME and ORACLE_HOME locations created in [Chapter 6, "Installing the Software for an Enterprise Deployment"](#) on a shared storage. WCPHOST1 and WCPHOST2 mount MW_HOME and use the existing Oracle WebLogic Server, Oracle SOA Suite, Oracle WebCenter Portal, and Oracle WebCenter Content binary installations.

If you have not done so already, install Oracle WebCenter Content binaries into the Middleware Home before adding Oracle WebCenter Content to the domain. For details, see [Section 6.3.2.3, "Installing Oracle WebCenter Content"](#).

Extend the domain to include Oracle WebCenter Content. [Table 13–1](#) lists the steps for configuring WebCenter Content and other tasks required for extending the domain with WebCenter Content managed servers.

Table 13–1 Steps for Extending the Domain with WebCenter Content

Step	Description	More Information
Extend the domain for WebCenter Content	Extend the WebLogic domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment"	Section 13.2, "Extending the Domain to Include Oracle WebCenter Content"
Propagate the domain configuration	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directories.	Section 13.3, "Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility"
Configure the load balancer to route WebCenter Content traffic	Configure your load balancer with a rule that specifies how to route WebCenter Content traffic.	Section 13.4, "Configuring the Load Balancer to Route WebCenter Content Traffic"
Start Node Manager on WCPHOST1 and WCPHOST2	Start Node Manager on WCPHOST1 and on WCPHOST2.	Section 13.5, "Starting Node Manager on WCPHOST1 and WCPHOST2"
Restart the Administration Server for the domain	Stop and then restart the Administration Server.	Section 13.6, "Restarting the Administration Server"
Start the first WebCenter Content managed server and configure its Content Server instance	Start the WLS_WCC1 managed server and complete the initial Content Server configuration.	Section 13.7, "Starting and Configuring the WLS_WCC1 Managed Server"
Propagate the changes in the cwallet.sso file back to the Administration Server.	Copy the updated cwallet.sso file to the Administration Server directory.	Section 13.8, "Updating the cwallet File in the Administration Server"
Start the second WebCenter Content managed server and configure its Content Server instance	Configure the WLS_WCC2 managed server and complete the initial Content Server configuration.	Section 13.9, "Starting and Configuring the WLS_WCC2 Managed Server"
Enable service retries after an Oracle RAC failover	Set the ServiceAllowRetry configuration parameter to true in the Content Server config.cfg file.	Section 13.10, "Configuring Service Retries for Oracle WebCenter Content"
Configure Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the managed servers, set the frontend HTTP host and port, and set the WLS Cluster address for WCC_Cluster.	Section 13.11, "Configuring Oracle HTTP Server for the WLS_WCC Managed Servers"

Table 13–1 (Cont.) Steps for Extending the Domain with WebCenter Content

Step	Description	More Information
Validate access to WebCenter Content through Oracle HTTP Server	Verify the URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCC_Cluster.	Section 13.12, "Validating Access Through Oracle HTTP Server"
Back up the WebCenter Content Configuration	Back up the newly extended domain configuration.	Section 13.13, "Backing Up the Installation"
Set up Oracle WebCenter Content Server for use with WebCenter Portal	Configure Oracle WebCenter Content Server for use with Oracle WebCenter Portal applications., such as Spaces.	Section 13.14, "Configure Oracle WebCenter Content for Oracle WebCenter Portal"
Register the Content Server with WebCenter Portal applications.	Connect WebCenter Portal applications, such as Spaces, to the Content Server.	Section 13.15, "Registering Oracle WebCenter Content with Oracle WebCenter Portal Applications"
Extend the domain for Inbound Refinery	Extend the WebLogic domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment" .	Section 13.16, "Installing and Configuring the Inbound Refinery"

13.2 Extending the Domain to Include Oracle WebCenter Content

You must extend the domain created in [Chapter 8, "Creating a Domain for an Enterprise Deployment"](#) to include Oracle WebCenter Content. Optionally, a new domain may be created containing only Oracle WebCenter Content.

Note: Before performing these steps, back up the domain as described in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain to include Oracle WebCenter Content:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, Oracle recommends that all instances are running, so that the validation check later on becomes more reliable.
2. Shut down all managed servers in the domain.
3. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard. This is within the Oracle Common home directory (notice that domain extensions are run from SOAHOST1 where the Administration Server resides).

```
cd ORACLE_COMMON_HOME/common/bin
```

4. Start the Configuration Wizard:

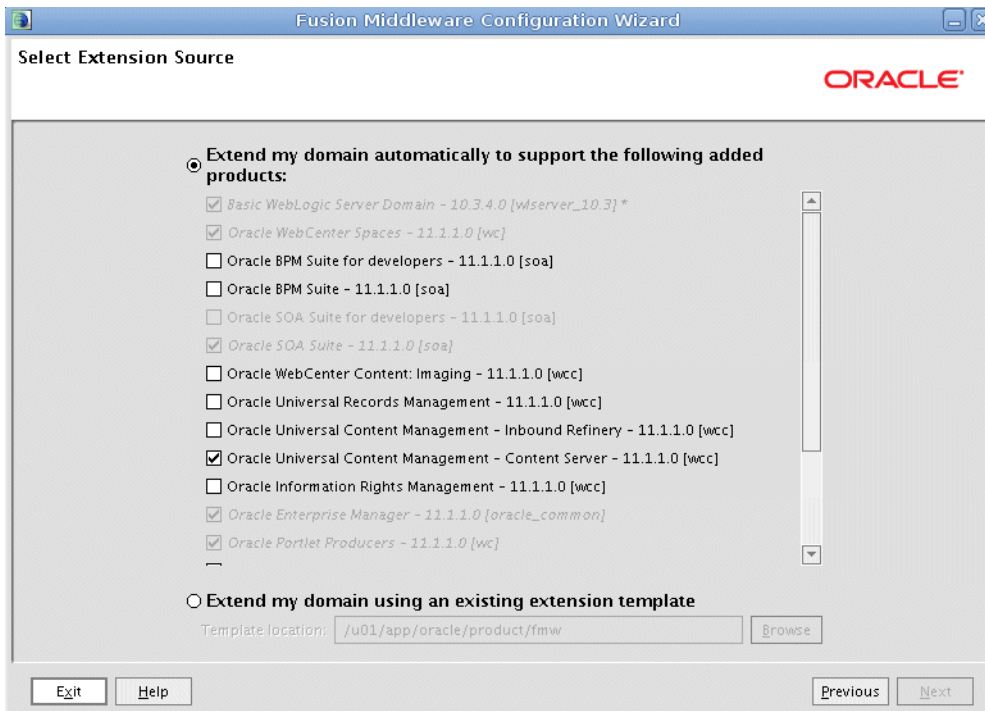
```
./config.sh
```

5. In the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.
6. In the WebLogic Domain Directory screen, select the **WebLogic domain directory** (`ORACLE_BASE/admin/domain_name/aserver/domain_name`), and click **Next**.
7. In the Select Extension Source screen, do the following (as shown in [Figure 13–1](#)):

- Select **Extend my domain automatically to support the following added products**.
 - Select the following product:
 - **Oracle Universal Content Management - Content Server - 11.1.1.0 wcc**
- Click **Next**.

Note: Do not select **Oracle Universal Content Management - Inbound Refinery - 11.1.1.0**. You will configure this feature later, as described in [Section 13.16.5, "Configuring Inbound Refinery"](#).

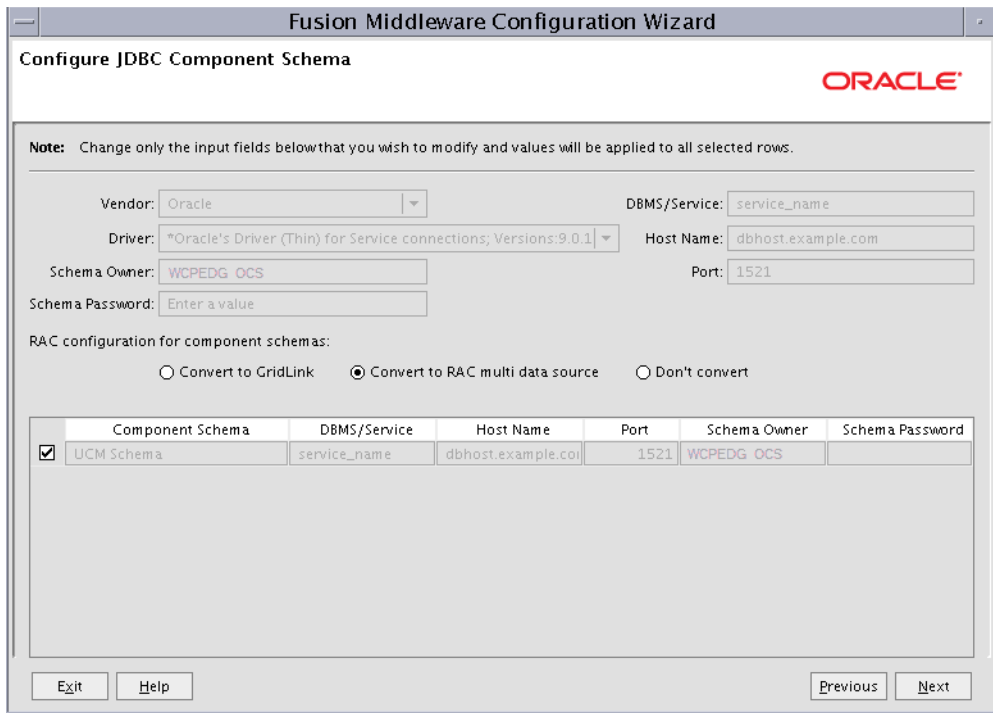
Figure 13–1 Select Extension Source screen for Oracle WebCenter Content



Screenshot of the Select Extension Source screen for Oracle WebCenter Content.

8. In the Configure JDBC Component Schema screen, do the following (as shown in [Figure 13–2](#)):
 - Select **UCM Schema**.
 - Select **Convert to RAC multi data source**.
- Click **Next**.

Figure 13–2 Configure JDBC Component Schema Screen for Oracle WebCenter Content



Configure JDBC Component Schema Screen for Oracle WebCenter Content

9. In the Configure RAC Multi Data Sources Component Schema screen, do the following (as shown in [Figure 13–3](#)):

- a. Select **UCM Schema**. Leave the other data sources as they are.
- b. Enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU:

Driver: Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, and later**.

Service Name: Enter the service name of the database (**wcpedg.mycompany.com**).

Username: Enter the complete user name (including the prefix) for the schemas.

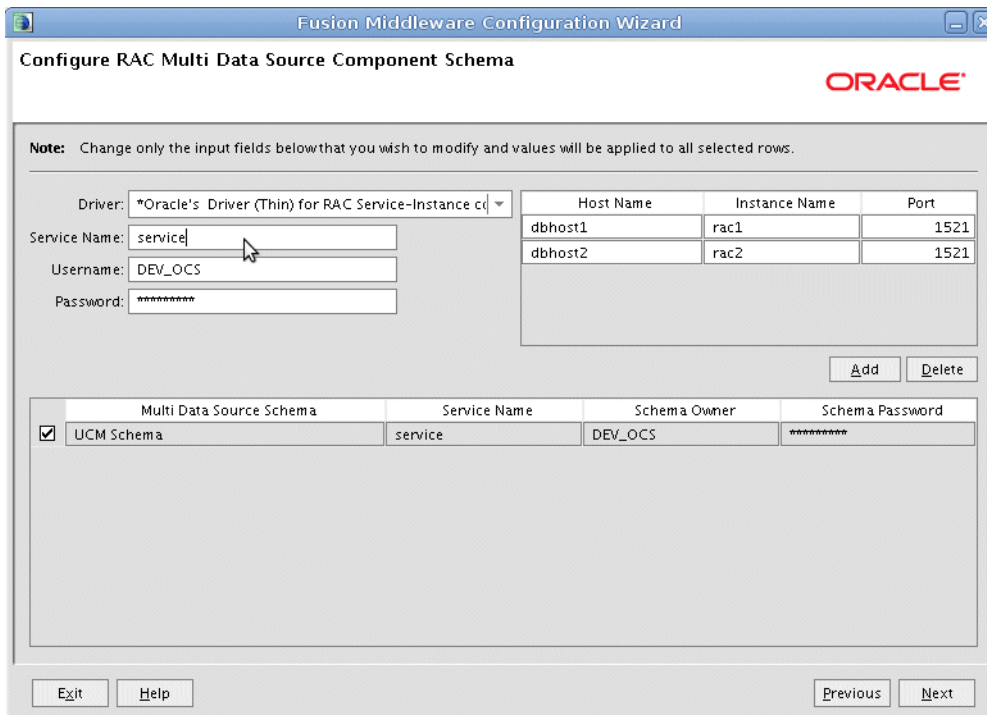
Password: Enter the password to use to access the schemas.

- c. Click **Add** and enter the details for the first Oracle RAC instance.
- d. Repeat step c for each Oracle RAC instance.

Note: Leave the SOA and WebCenter Portal schemas as they are.

- e. Click **Next**.

Figure 13–3 Configure RAC Multi Data Source Component Schema Screen for Oracle WebCenter Content



Configure RAC Multi Data Source Component Schema Screen for Oracle WebCenter Content

10. In the Test JDBC Data Sources screen, the connections should be tested automatically. The **Status** column displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen and correct your entries.

Click **Next** when all the connections are successful.

11. In the Optional Configuration screen, select the following:

- **Managed Servers, Clusters and Machines**
- **Deployment and Services**

Click **Next**.

12. In the Configure Managed Servers screen, click **Add** to add the required managed servers as shown in [Table 13–2](#). Do not modify the other servers that appear in this screen; leave them as they are.

Table 13–2 Managed Servers

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_WCC1	WCPHOST1	16200	n/a	No
WLS_WCC2	WCPHOST2	16200	n/a	No

Click **Next**.

13. In the Configure Clusters screen, click **Add** to add the clusters as shown in [Table 13-3](#). Do not modify the other clusters that appear in this screen; leave them as they are.

Table 13-3 Clusters

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
WCC_Cluster	unicast	n/a	n/a	Leave it empty.

Click **Next**.

14. In the Assign Servers to Clusters screen, add the following. Do not modify the other assignments that appear in this screen; leave them as they are.
 - WCC_Cluster
 - WLS_WCC1
 - WLS_WCC2

Click **Next**.

15. In the Configure Machines screen, click the **Unix Machine** tab and add the following two new machines:

Table 13-4 Machines

Name	Node Manager Listen Address
WCPHOST1	WCPHOST1
WCPHOST2	WCPHOST2

Leave all other fields to their default values. Click **Next**.

16. In the Assign Servers to Machines screen, assign servers to machines as follows:
 - Assign WLS_WCC1 to WCPHOST1.
 - Assign WLS_WCC2 to WCPHOST2.

Click **Next**.

17. In the Target Deployments to Clusters or Servers screen, click **Next**.
18. In the Target Services to Clusters or Servers screen, click **Next**.
19. In the Configuration Summary screen, click **Extend**.
20. Click **OK** in the warning dialog about conflicts in ports for the domain.
21. In the Creating Domain screen, click **Done**.
22. Start the Administration Server to make these changes to take effect. See [Section 13.6, "Restarting the Administration Server."](#)

13.3 Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility

To propagate the domain configuration:

1. Run the `pack` command on SOAHOST1 to create a template pack as follows:

```
cd ORACLE_COMMON_HOME/common/bin
./pack.sh -managed=true -domain=ORACLE_BASE/admin/
domain_name/aserver/domain_name -template=edgdomaintemplateWCC.jar -template_
name=edgdomaintemplateWCC
```

2. Run the following command on SOAHOST1 to copy the template pack created in the previous step to WCPHOST1 and WCPHOST2:

Note: Assuming that WCPHOST1 shares the ORACLE_HOME with WCPHOST2, the template will be present in the same directory in WCPHOST2; otherwise, copy it also to WCPHOST2.

```
scp edgdomaintemplateWCC.jar oracle@WCPHOST1:ORACLE_BASE/product/fmw/oracle_
common/common/bin
```

```
scp edgdomaintemplateWCC.jar oracle@WCPHOST2:ORACLE_BASE/product/fmw/oracle_
common/common/bin
```

3. Run the unpack command on WCPHOST1 and WCPHOST2 to unpack the propagated template.

Note: Make sure to run the unpack command from the ORACLE_COMMON_HOME/common/bin directory, not from WL_HOME/common/bin.

```
WCPHOST1> cd ORACLE_COMMON_HOME/common/bin
WCPHOST1> ./unpack.sh -domain=ORACLE_BASE/admin/domain_name
/mserver/domain_name -template=edgdomaintemplateWCC.jar -app_dir=ORACLE_BASE
/admin/domain_name/mserver/applications
```

```
WCPHOST2> cd ORACLE_COMMON_HOME/common/bin
WCPHOST2> ./unpack.sh -domain=ORACLE_BASE/admin/domain_name
/mserver/domain_name -template=edgdomaintemplateWCC.jar -app_dir=ORACLE_BASE
/admin/domain_name/mserver/applications
```

Note: The ORACLE_BASE/admin/domain_name/mserver directory must exist before running unpack. In addition, the ORACLE_BASE/admin/domain_name/mserver/applications must be empty.

13.4 Configuring the Load Balancer to Route WebCenter Content Traffic

In this WebCenter Portal enterprise deployment, the Load Balancer load-balances traffic across both Content Servers. The Load Balancer, forwards the socket connection from WebCenter Portal applications to one of the Content Servers (on WCPHOST1 or WCPHOST2). Since the connection is persistent, one Content Server receives most of the traffic, if not all. The other Content Server functions as a failover server in case the primary server is not available.

You must configure your Load Balancer with a rule that specifies how to route WebCenter Content traffic, for example:

- (LBR)10.110.10.135:4444 -> 10.110.10.23:4444 (WCPHOST1) -> 10.110.10.24:4444 (WCPHOST2)

13.5 Starting Node Manager on WCPHOST1 and WCPHOST2

Perform these steps to start Node Manager on WCPHOST1 and WCPHOST2 if Node Manager has not started already:

1. On both WCPHOST1 and WCPHOST2, run the `setNMProps.sh` script, which is located in the `ORACLE_COMMON_HOME/common/bin` directory, to set the `StartScriptEnabled` property to 'true' before starting Node Manager:

```
WCPHOSTn> cd ORACLE_COMMON_HOME/common/bin
WCPHOSTn> ./setNMProps.sh
```

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

Note: If the Oracle WebCenter Content Server is sharing the `MW_HOME` in a local or shared storage with SOA and WebCenter Portal, as suggested in the shared storage configuration described in [Chapter 3, "Preparing the Network for an Enterprise Deployment,"](#) it is not required to run `setNMProps.sh` again. In this case, Node Manager has already been configured to use a start script.

2. Run the following commands on both WCPHOST1 and WCPHOST2 to start Node Manager:

```
WCPHOSTn> cd WL_HOME/server/bin
WCPHOSTn> ./startNodeManager.sh
```

13.6 Restarting the Administration Server

Restart the Administration Server for these changes take effect. To restart the Administration Server, stop it first using the Administration Console and then start it again as described in [Chapter 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

13.7 Starting and Configuring the WLS_WCC1 Managed Server

This section describes how to start the new WLS_WCC1 managed server and how to configure the Content Server (on WLS_WCC1) for the WebCenter Portal enterprise deployment.

Note: In this WebCenter Portal enterprise deployment, the Load Balancer balances traffic across both Content Servers. If you have not done so already, configure your Load Balancer with a rule that specifies how to route WebCenter Content traffic. For details, see [Section 13.4, "Configuring the Load Balancer to Route WebCenter Content Traffic"](#).

Starting the WLS_WCC1 Managed Server

To start the WLS_WCC1 managed server:

1. Start the WLS_WCC1 managed server using the Oracle WebLogic Server Administration Console as follows:

- a. Expand the **Environment** node in the Domain Structure window.
 - b. Choose **Servers**.
 - c. On the Summary or Servers page, click the **Control** tab.
 - d. Select **WLS_WCC1**, and then click **Start**.
2. 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

Configuring the Content Server (on WLS_WCC1 Managed Server)

To configure the Content Server:

1. Log in to Content Server at `http://wcpinternal.mycompany.com/cs` using your Oracle WebLogic administration user name and password to display a configuration page.

Note: The Oracle WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location for the Oracle WebCenter Portal enterprise deployment is at `ORACLE_BASE/admin/wc_domain/WCC_Cluster`.

2. Change the following values on the server configuration page (make sure to select the **Is New Content Server Instance** check box to see all options):
 - **Content Server Instance Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs`.
 - **Native File Repository Location:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/vault`.
 - **WebLayout Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/weblayout`.
 - **User Profile Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/data/users/profiles`.
 - **Server Socket Port:** Set this to 4444.
 - **Incoming Socket Connection Address Security Filter:** Set this to a pipe-delimited list of localhost and the server IPs:
`127.0.0.1|WCPHOST1_IP_Address|WCPHOST2_IP_Address|WEBHOST1_IP_Address|WEBHOST2_IP_Address`

Note: For this step, use IP addresses, not hostnames.

- **WebServer HTTP/HTTPS Address:** Set this to `wcpinternal.mycompany.com`.
Enter the Load Balancer address here so that requests to `/cs` can use any available Content Server node.

Note: If you have not done so already, add a rule to your Load Balancer that specifies how to route WebCenter Content traffic, for example:

- (LBR)10.110.10.135:4444 -> 10.110.10.23:4444 (WCPHOST1) -> 10.110.10.24:4444 (WCPHOST2)
-
-

- **Web Address is HTTPS:** Deselect (*uncheck*) this check box.
 - **Server Instance Label:** Set this to WCC_Cluster1.
 - **Server Instance Description:** Set this to Cluster WCC_Cluster1.
 - **Auto_Number Prefix:** Set this to WCC_Cluster1-
3. Click **Submit** when finished, and restart the managed server using the Oracle WebLogic Server Administration Console.

13.8 Updating the cwallet File in the Administration Server

The Oracle WebCenter Content server updates the `cwallet.sso` file located in `ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig` when it starts. You must propagate this change back to the Administration Server. To do this, copy the file to `ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig` in SOAHOST1 using the following command (all on a single line):

```
WCPHOST1> scp ORACLE_BASE/admin/domain_name/mserver/
domain_name/config/fmwconfig/cwallet.sso oracle@SOAHOST1:ORACLE_
BASE
/admin/domain_name/aserver/domain_name/config/fmwconfig/
```

Note: If any operation is performed in the WLS_WCC n servers that modifies the `cwallet.sso` file in the `ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig` directory, the file must be immediately copied to the Administration Server domain directory on SOAHOST1 at `ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig`.

13.9 Starting and Configuring the WLS_WCC2 Managed Server

Starting the WLS_WCC2 Managed Server

Start the WLS_WCC2 managed server using the Oracle WebLogic Server Administration Console as follows:

1. Using the Oracle WebLogic Server Administration Console as follows:
 - a. Expand the **Environment** node in the Domain Structure window.
 - b. Choose **Servers**.
 - c. On the Summary of Servers page, click the **Control** tab.
 - d. Select **WLS_WCC2** and then click **Start**.

2. 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 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#) for possible causes.

Configuring the WLS_WCC2 Managed Server

To configure the WLS_WCC2 managed server:

1. Log in to WLS_WCC2 at `http://WCPHOST2:16200/cs` using your Oracle WebLogic administration user name and password to display a configuration page:

Note: The WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location for the Oracle WebCenter Portal enterprise deployment is at `ORACLE_BASE/admin/wc_domain/WCC_Cluster`.

2. Change the following values on the server configuration page:
 - **Content Server Instance Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs`
 - **Native File Repository Location:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/vault`
 - **WebLayout Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/weblayout`
 - **User Profile Folder:** Set this to `ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/data/users/profiles`.
3. Make sure that the **Is new Content Server Instance?** check box is **not** selected.
4. Click **Submit** when finished and restart the managed server using the Oracle WebLogic Server Administration Console.

13.10 Configuring Service Retries for Oracle WebCenter Content

Set the following parameter in Oracle Content Server's `config.cfg` file in order to enable log in retries during an Oracle RAC failover:

```
ServiceAllowRetry=true
```

If this value is not set, you are required to manually retry any operation that was in progress when the failover began.

To add the `ServiceAllowRetry` configuration parameter for Oracle WebCenter Content:

1. Go to the WebLogic Server Administration Console for Oracle WebCenter Content at `http://WCPHOST1:16200/cs`, and log in using your Oracle WebLogic administration user name and password.
2. Open the Administration page, and then choose **Admin Server**.
3. On the Content Admin Server page, click **General Configuration** on the left.
4. On the General Configuration page, add the following parameter in the **Additional Configuration Variables** box:

```
ServiceAllowRetry=true
```

5. Click **Save** and restart all WebCenter Content managed servers (WLS_WCC n).

Note: The new parameter is included in the `config.cfg` file, which is at the following location:

```
ORACLE_BASE/admin/wc_domain/WCC_Cluster/cs/config/config.cfg
```

You can also edit this file directly in a text editor. Do not forget to restart all WebCenter Content managed servers.

13.11 Configuring Oracle HTTP Server for the WLS_WCC Managed Servers

To enable Oracle HTTP Server to route to WCC_Cluster, which contains the WLS_WCC1 and WLS_WCC2 managed servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster:

1. On WEBHOST1 and WEBHOST2, add the following lines to the `ORACLE_BASE/admin/instance_name/config/OHS/component_name/mod_wl_ohs.conf` file:

```
#Oracle WebCenter Content

<Location /cs>
  WebLogicCluster WCPHOST1:16200,WCPHOST2:16200
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

<Location /adfAuthentication>
  WebLogicCluster WCPHOST1:16200,WCPHOST2:16200
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

<Location /_ocsh>
  WebLogicCluster WCPHOST1:16200,WCPHOST2:16200
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
```

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2.

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

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

13.12 Validating Access Through Oracle HTTP Server

Verify the following URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCC_Cluster:

1. While WLS_WCC2 is running, stop WLS_WCC1 using the Oracle WebLogic Server Administration Console.
2. Access `http://WEBHOST1:7777/cs` to verify it is functioning properly.
3. Start WLS_WCC1 from the Oracle WebLogic Server Administration Console.
4. Stop WLS_WCC2 from the Oracle WebLogic Server Administration Console.
5. Access `http://WEBHOST1:7777/cs` to verify it is functioning properly.

13.13 Backing Up the Installation

After you have verified that the extended 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. You can discard this backup once the enterprise deployment setup is complete. At that point, the regular deployment-specific backup and recovery process can be initiated. 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 that guide. For information on how to recover components, see the "Recovery of Components" and "Recovery After Loss of Component" sections in the guide. For recommendations specific to recovering from the loss of a host, see the "Recovering Oracle HTTP Server to a Different Host" section in the guide. Also refer to the Oracle Database Backup and Recovery Guide *Oracle Database Backup and Recovery User's Guide* for information on database backup.

To back up the installation:

1. Back up the web tier. Run the commands from SOAHOST1:
 - a. Shut down the instance using `opmnctl`.

```
ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
```
 - 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 Oracle Instance Home on the web tier using the following command:

```
tar -cvpf BACKUP_LOCATION/web_instance_name.tar ORACLE_INSTANCE
```
 - d. Start the instance using `opmnctl`:

```
cd ORACLE_BASE/admin/instance_name/bin
opmnctl startall
```
2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or operating system tools such as `tar` for cold backups if possible.

3. Back up the Administration Server domain directory to save your domain configuration. The configuration files all exist in the `ORACLE_BASE/admin/domain_name` directory:

Run the following command to create the backup:

```
SOAHOST1> tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

13.14 Configure Oracle WebCenter Content for Oracle WebCenter Portal

This section describes tasks required for configuring Oracle WebCenter Content Server for use with Oracle WebCenter Portal. This section includes the following:

- [Section 13.14.1, "Enabling Mandatory Content Server Components \(Folders_g and WebCenterConfigure\)"](#)
- [Section 13.14.2, "Enabling and Configuring the Dynamic Converter Component"](#)
- [Section 13.14.3, "Configuring Additional Content Server Features"](#)

13.14.1 Enabling Mandatory Content Server Components (Folders_g and WebCenterConfigure)

Mandatory

For WebCenter Portal, you must enable the following Content Server components:

- **Folders_g** - provides a hierarchical folder interface to content in Content Server
- **WebCenterConfigure** - configures an instance of Content Server for WebCenter Portal applications

For WebCenter Portal, you must disable the following Content Server components:

- **FrameworkFolders** - this component is not compatible with the **Folders_g**

For detailed steps, see "Enabling Mandatory Components" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

Note: If Folder_g is not enabled, the following exception displays:

```
SEVERE: UCM feature folders is not installed on server. at
oracle.webcenter.content.integration.spi.ucm.UCMBridge.getBridge(UC
MBridge.java:349) ....
```

To enable required components:

1. Log in to Oracle WebCenter Content Administration.
2. Navigate to **Administration, Admin Server, Component Manager** and then enable/disable.
3. Disable **FrameworkFolders**.
4. Enable **Folders_g** and **WebCenterConfigure**.
5. Click **Save/Update** at the bottom.
6. Restart Content Server. Optionally, Content Server may be restarted after all the configuration steps have been completed.

13.14.2 Enabling and Configuring the Dynamic Converter Component

Optional, but strongly recommended

This configuration is required for the Slide Previewer capability in WebCenter Portal, which makes use of the HTML renditions generated on the fly by the Dynamic Converter.

The configuration for the Dynamic Converter consists of two steps: enabling the Dynamic Converter, and defining the file types for which the Dynamic Converter is available. For detailed steps, see "Configuring the Dynamic Converter Component" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

13.14.3 Configuring Additional Content Server Features

There are several other Content Server features that, while not mandatory, can provide additional functionality in WebCenter Portal applications. For example, you can enable features such as Site Studio, OracleTextSearch, and so on. To find out more, and for detailed steps, see "Configuration Roadmap for Content Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

13.15 Registering Oracle WebCenter Content with Oracle WebCenter Portal Applications

To register Oracle WebCenter Content Server with a WebCenter Portal application, such as Spaces:

Note: For more information about Content Server registration, see "Managing Content Repositories" of the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

1. Log in to Enterprise Manager Fusion Middleware Control and navigate to the home page for your application.
For example, to navigate to the home page for Spaces, expand **WebCenter > Portal > Spaces**
2. From the **WebCenter Portal** menu, choose **Settings**, and then **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Content Repository**.
4. To connect to a new content repository, click **Add**.
5. Enter a unique name for this connection, specify the content repository type, and indicate whether this connection is the active (or default) connection for the application.
 - **Connection Name**
Enter a unique name for this content repository connection. The name must be unique (across all connection types) within the WebCenter Portal application.
 - **Repository Type**
Choose the type of repository to which you want to connect: **Oracle Content Server**.
 - **Active Connection**

Make this the default content repository for your WebCenter Portal application.

You can connect your WebCenter Portal application to multiple content repositories; all connections are used. One connection must be designated the default (or active) connection.

6. For the Spaces application only, enter additional content repository details:

■ **Content Administrator**

Enter a user name with administrative rights for this Content Server instance. This user is used to create and maintain folders for Spaces content and manage content access rights. Defaults to `sysadmin`. Administrative privileges are required for this connection so that operations can be performed on behalf of Spaces users.

■ **Root Folder**

Enter the root folder under which all Spaces content is stored. Specify a content repository folder that does not yet exist and use the format: `/foldername`. For example: `/MyWebCenterSpaces`. The Root Folder cannot be `/`, the root itself, and it must be unique across applications. The folder specified is created for you when the application starts up.

■ **Application Name**

Enter a unique name for this Spaces application within this content repository. For example: **MySpacesApp**

The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to thirty characters.

This name is used to separate data when multiple Spaces applications share the same content repository and should be unique across applications.

7. Enter connection details for the content repository:

■ **RIDC Socket Type**

Choose **Socket** - Uses an intradoc socket connection to connect to Content Server. The client IP address must be added to the list of authorized addresses in the Content Server. In this case, the client is the machine on which Oracle WebCenter Portal is running.

■ **Server Host**

Enter the Load Balancer address, **wcpinternal.mycompany.com**, so that requests to `/cs` use any available Content Server node.

Note: If you have not done so already, add a rule to your Load Balancer that specifies how to route WebCenter Content traffic, for example:

- (LBR)10.110.10.135:4444 -> 10.110.10.23:4444 (WCPHOST1) -> 10.110.10.24:4444 (WCPHOST2)
-

■ **Server Port**

Enter the port on which the Content Server listens: **4444**

■ **Connection Timeout (ms)**

Specify the length of time allowed to log in to Content Server (in milliseconds) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation. Choose a reasonable timeout depending on your environment. For example: **30000**.

- **Authentication Method**

Choose **Identity Propagation** - In this enterprise deployment, Content Server and the WebCenter Portal application both use the same identity store to authenticate users.

- **Web Context Root**

Enter `/cs` as the Web server context root for Content Server.

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the managed server on which the WebCenter Portal application is deployed.

13.16 Installing and Configuring the Inbound Refinery

The Inbound Refinery (IBR) is required for Document Conversion by Oracle WebCenter Content.

For availability reasons, Oracle recommends installing at least two inbound refineries, each installed on a separate machine. Within the WebCenter Portal enterprise deployment topology, inbound refinery is installed on the same machine as Oracle Webcenter Content Server.

Even though a cluster is created in the process of extending the domain with Inbound Refinery, it is worth noting that all Inbound Refinery instances are completely independent. Clustering is used for management purposes only.

This section includes the following topics:

- [Section 13.16.1, "Extending the Domain to Include Inbound Refinery"](#)
- [Section 13.16.2, "Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility"](#)
- [Section 13.16.3, "Restarting the Administration Server"](#)
- [Section 13.16.4, "Starting the Inbound Refinery Managed Servers"](#)
- [Section 13.16.5, "Configuring Inbound Refinery"](#)

13.16.1 Extending the Domain to Include Inbound Refinery

You must extend the domain created in [Section 8, "Creating a Domain for an Enterprise Deployment"](#) to include Oracle WebCenter Content: Inbound Refinery.

Note: Before performing these steps, back up the domain as described in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain to include Oracle WebCenter Content: Inbound Refinery:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, Oracle recommends that all instances are running, so that the validation check later on becomes more reliable.
2. Shut down all managed servers in the domain.

3. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard. This is within the Oracle Common home directory (notice that domain extensions are run from SOAHOST1 where the Administration Server resides).

```
cd ORACLE_COMMON_HOME/common/bin
```

4. Start the Configuration Wizard:

```
./config.sh
```

5. In the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.
6. In the WebLogic Domain Directory screen, select the WebLogic domain directory (`ORACLE_BASE/admin/domain_name/aserver/domain_name`), and click **Next**.
7. In the Select Extension Source screen, do the following:
 - Select **Extend my domain automatically to support the following added products**.
 - Select the following product:
 - **Oracle Universal Content Management - Inbound Refinery - 11.1.1.0 [wcc]**

Click **Next**.

8. In the Configure JDBC Component Schema screen, nothing needs to be done. Inbound refineries do not have a schema in the database. Click **Next** to continue.
9. In the Optional Configuration screen, select the following:
 - **Managed Servers, Clusters and Machines**
 - **Deployment and Services**

Click **Next**.

10. In the Configure Managed Servers screen, add the required managed servers.

A server is created automatically. Rename this server to WLS_IBR1 and add a new server called WLS_IBR2. Give these servers the attributes listed in [Table 13–5](#). Do not modify the other servers that are shown in this screen; leave them as they are.

Table 13–5 Managed Servers

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_IBR1	WCPHOST1	16250	n/a	No
WLS_IBR2	WCPHOST2	16250	n/a	No

Click **Next**.

11. In the Configure Clusters screen, click **Add** to add the clusters as shown in [Table 13–6](#). Do not modify the other clusters that appear in this screen; leave them as they are.

Table 13–6 Clusters

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
IBR_Cluster	unicast	n/a	n/a	Leave empty

Click **Next**.

Note: All Inbound Refinery instances are completely independent. The cluster is used for management purposes only.

12. In the Configure Machines screen, click **Next**.
13. In the Assign Servers to Machines screen, assign servers to machines as follows:
 - Assign **WLS_IBR1** to **WCPHOST1**.
 - Assign **WLS_IBR2** to **WCPHOST2**.

Click **Next**.

14. In the Target Deployments to Clusters or Servers screen, ensure the following targets:
 - **usermessagingserver** and **usermessagingdriver-email** should be targeted only to **SOA_Cluster**. (The **usermessaging-xmpp**, **usermessaging-smpp**, and **usermessaging-voicexml** applications are optional.)
 - **WSM-PM** should be targeted only to **SOA_Cluster**.
 - The **oracle.rules***, **oracle.sdp.***, **oracle.soa.workflow.wc**, and **oracle.soa.*** deployments should be targeted to **SOA_Cluster** only.
 - The **oracle.wsm.seedpolicies** library should be targeted to **SOA_Cluster** (and any servers expected to host WSM-PM protected web services).

Click **Next**.

15. In the Target Services to Clusters or Servers screen, click **Next**.
16. In the Configuration Summary screen, click **Extend**.
17. In the Creating Domain screen, click **Done**.
18. Start the Administration Server to make these changes to take effect. See [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

13.16.2 Propagating the Domain Configuration to WCPHOST1 and WCPHOST2 Using the unpack Utility

To propagate the domain configuration:

1. Run the `pack` command on SOAHOST1 to create a template pack using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name
-template=edgdomaintemplateIBR.jar -template_name=edgdomain_templateIBR
```

2. Run the following command on SOAHOST1 to copy the template pack created in the previous step to WCPHOST2:

Note: Assuming that WCPHOST1 shares the ORACLE_HOME with SOAHOST1, the template will be present in the same directory in WCPHOST1; otherwise, copy it also to WCPHOST1.

```
scp edgdomaintemplateIBR.jar oracle@WCPHOST2:ORACLE_BASE/product/fmw/oracle_
common/common/bin
```

3. Run the `unpack` command on WCPHOST1 to unpack the propagated template.

Note: Make sure to run `unpack` from the `ORACLE_COMMON_HOME/common/bin` directory, not from `WL_HOME/common/bin`.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=ORACLE_BASE/admin/domain_name/msserver/domain_name
-template=edgdomaintemplateIBR.jar
-app_dir=ORACLE_BASE/admin/domain_name/msserver/applications
-overwrite_domain=true
```

Note: The `ORACLE_BASE/admin/domain_name/msserver` directory must exist before running `unpack`. In addition, the `ORACLE_BASE/admin/domain_name/msserver/applications` must be empty.

4. Repeat step 3 for WCPHOST2.

13.16.3 Restarting the Administration Server

Restart the Administration Server to make these changes take effect. To restart the Administration Server, stop it first using the Administration Console and then start it again as described in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

13.16.4 Starting the Inbound Refinery Managed Servers

To start the WLS_IBR1 on WCPHOST1 and WLS_IBR2 managed server on WCPHOST2:

1. Log in to the Oracle WebLogic Server Administration Console at:
`http://ADMINVHN:7001/console`
2. In the Domain Structure window, expand the **Environment** node and then select **Servers**.
3. On the Summary of Servers page, open the **Control** tab.
4. Select WLS_IBR1 and WLS_IBR2 from the **Servers** column of the table.
5. Click **Start**.

13.16.5 Configuring Inbound Refinery

An inbound refinery needs to be accessed only once through HTTP in order to initialize its configuration. This can be done directly, at the managed server's listen address. An inbound refinery should not be placed behind an HTTP server.

All subsequent access to an inbound refinery is through the socket listener. This listener is protected through the incoming socket connection address security filter configured in the next section.

Oracle recommends configuring each Oracle WebCenter Content Server with all inbound refineries. The process for configuring Oracle WebCenter Content is to add an

inbound refinery as a provider. There are also post-installation steps that must be performed with the inbound refinery.

The following sections describe the procedures for post-installation configuration of Inbound Refinery:

- [Section 13.16.5.1, "Configuring Inbound Refinery Settings"](#)
- [Section 13.16.5.2, "Configuring Document Conversion"](#)
- [Section 13.16.5.3, "Configuring Oracle WebCenter Content with the Inbound Refinery"](#)

13.16.5.1 Configuring Inbound Refinery Settings

To configure the Inbound Refinery settings:

1. Access the Inbound Refinery post-installation configuration screen at the following URL:

```
http://WCPHOST1:16250/ibr/
```

2. In the configuration screen, set the configuration settings as follows:

- **Inbound Refinery Instance Folder:** Set this to *ORACLE_BASE/admin/wc_domain/WCC_Cluster/ibr1*. The directory path should be on a shared disk, but should be unique for each Inbound Refinery instance.
- **Native File Repository Location:** Set this to *ORACLE_BASE/admin/wc_domain/WCC_Cluster/ibr1/vault*.
- **WebLayout Folder:** Set this to *ORACLE_BASE/admin/wc_domain/WCC_Cluster/ibr1/weblayout*.
- **User Profile Folders:** Set this to *ORACLE_BASE/admin/wc_domain/WCC_Cluster/ibr1/data/users/profiles*.
- **Socket Connection Address Security Filter:** Set this to a pipe-delimited list of localhost and the server IPs:

```
127.0.0.1|WCPHOST1-IP|WCPHOST2-IP|WEBHOST1-IP|WEBHOST2-IP
```

This enables access from Oracle WebCenter Content Server. The values for *WCPHOST1-IP* and *WCPHOST2-IP* should be the IP addresses of the machines with the Oracle WebCenter Content Server instance or instances that will send jobs to Inbound Refinery, not necessarily the IP address of Inbound Refinery. (In the reference topology used in this enterprise deployment guide, however, these IP addresses are the same.)

This field accepts wildcards in the value; for example, *192.0.2.**. You can change this value later by setting `SocketHostAddressSecurityFilter` in *ORACLE_BASE/admin/domain_name/mserver/domain_name/ucm/ibr/config/config.cfg* and restarting Inbound Refinery.

- **Server Socket Port:** Enter an unused port number, such as 5555. This value is the number of the port for calling top-level services. Changing this field value changes the `IntradocServerPort` entry in *ORACLE_BASE/admin/domain_name/mserver/domain_name/ucm/ibr/config/config.cfg*. Take note of the port number as you need it later when configuring Oracle WebCenter Content.
- **Server Instance Name:** Specify a name for the Inbound Refinery server instance. You can accept the default or change it to a more useful name if you

want. Take note of the server name as you need it later when configuring Oracle WebCenter Content.

You can leave all other fields on the configuration page as they are.

3. Restart the Inbound Refinery managed server.
4. Repeat these steps for all the inbound refineries, using different names for the content folders.

For Inbound Refinery to work properly, you must specify the path to fonts used to generate font images. By default, the font path is set to the font directory in the JVM used by Inbound Refinery: *MW_HOME/jdk160_version/jre/lib/fonts*. However, the fonts included in the default directory are limited and may cause poor renditions. Also, in some cases if a non-standard JVM is used, then the JVM font path may be different than that specified as the default. If this is the case, an error message is displayed from both Inbound Refinery and Content Server. If this occurs, ensure the font path is set to the directory containing the fonts necessary to properly render your conversions. For more information, see "Specifying the Font Path" in the *Oracle WebCenter Content Administrator's Guide for Conversion*.

13.16.5.2 Configuring Document Conversion

To configure document conversion:

1. Log in to Inbound Refinery at the following URL:
`http://WCPHOST1:16250/ibr/`
2. Enable conversion components on Inbound Refinery. The core Inbound Refinery converts files to TIFF web-viewable files and JPEG image thumbnails. To use additional conversion types, you need to enable the necessary components:

Note: For information about the conversion components, see "Inbound Refinery Conversion Options and Related Components" in *Oracle Fusion Middleware Administrator's Guide for Conversion*.

- a. Open the **Administration** tray or menu, then choose **Admin Server**, and then **Server Features**.
 - b. Select the components you want. For more information, consult the readme files and the documentation for each component.
 - c. Click **Update**.
 - d. Click **OK** to enable the components.
 - e. Restart the Inbound Refinery managed server.
3. Enable PDFExportConverter in Inbound Refinery. PDFExportConverter uses Outside In to convert documents directly to PDF files. The conversion can be cross-platform and does not require any third-party product. You can enable PDFExportConverter for Inbound Refinery as a server feature:
 - a. Open the **Administration** tray or menu, then choose **Admin Server**, and then **Server Features**.
 - b. Select **PDFExportConverter**.
 - c. Click **Update**.
 - d. Click **OK** to enable this feature.

- e. Restart the Inbound Refinery managed server.
4. Set the primary web-viewable conversion to PDF Export:
 - a. Select **Conversion Settings**, then select **Primary Web Rendition**.
 - b. On the Primary Web-Viewable Rendition page, select **Convert to PDF using PDF Export**.
 - c. Click **Update** to save your changes.

Inbound Refinery will now use Outside In PDF Export to convert files directly to PDF without the use of third-party applications.

5. Restart the Administration Server and all Inbound Refinery managed servers.

13.16.5.3 Configuring Oracle WebCenter Content with the Inbound Refinery

Log into Oracle WebCenter Content:

1. Select **Administration**, and then **Providers**.
2. In the Create a New Provider section of the Providers page, click **Add** in the **outgoing** row.
3. Enter the details for your IBR instance, including, name, description, host, server port (IBRs intradoc port), context root, and instance name.

- **Provider Name:** Any short name with no spaces. It is a good idea to use the same value as the **Instance Name** value

The IBR instance name is obtained from the IBR server. To find the instance name, log into the IBR and select **Administration**, and then **Configuration for instanceName**.

Note: if you miss this step, you will not see the **Refinery Administration** menu item in the **Administration** menu.

- **Provider Description:** Any text string.
 - **Server Host Name:** The name of the host machine where the Inbound Refinery instance is running: WCCHOST1.
 - **HTTP Server Address:** The address of the Inbound Refinery instance: WCCHOST1:16250.
 - **Server Port:** The value of the Server Socket Port field for the Inbound Refinery instance as specified in [Section 13.16.5.1, "Configuring Inbound Refinery Settings."](#), for example 5555. This is the IntradocServerPort value in the Content Server's config.cfg file.
 - **Instance Name:** The server instance name for Inbound Refinery as specified in [Section 13.16.5.1, "Configuring Inbound Refinery Settings."](#) This is the IDC_Name value in the Content Server's config.cfg file.
 - **Relative Web Root:** The web root of the Inbound Refinery instance: /ibr/.
4. Under Conversion Options, check **Handles Inbound Refinery Conversion Jobs**. Do *not* check **Inbound Refinery Read Only Mode**.
 5. Click **Add**.
 6. Restart Oracle WebCenter Content Server.

7. Select the file types to be sent to the IBR:
 - a. Select **Administration**, **Refinery Administration** and then **File Formats Wizard**.
 - b. Check the boxes for the appropriate file types to send to the refinery.

Do *not* check **HTML**, and also do not check **wiki** and **blog** unless you have enabled their conversion through the **WebCenterConversions** component. See also, "Selecting the File Formats To Be Converted" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

8. Enable wiki and blog conversion to PDF.

For details, see "Enabling the Conversion of Wikis and Blogs into PDFs" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

Configuring Server Migration for an Enterprise Deployment

This chapter describes the procedures for configuring server migration for the enterprise deployment.

This chapter contains the following sections:

- [Section 14.1, "Overview of Server Migration for an Enterprise Deployment"](#)
- [Section 14.2, "Setting Up a User and Tablespace for the Server Migration Leasing Table"](#)
- [Section 14.3, "Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console"](#)
- [Section 14.4, "Enabling Host Name Verification Certificates between SOAHOST1 and SOAHOST2 and the Administration Server"](#)
- [Section 14.5, "Editing the Node Manager's Properties File"](#)
- [Section 14.6, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"](#)
- [Section 14.7, "Configuring Server Migration Targets"](#)
- [Section 14.8, "Testing Server Migration"](#)

14.1 Overview of Server Migration for an Enterprise Deployment

Configure server migration for the *WLS_SOA1* and *WLS_SOA2* managed servers. With server migration configured, should failure occur, the *WLS_SOA1* managed server restarts on *SOAHOST2*, and the *WLS_SOA2* managed server restarts on *SOAHOST1*. The *WLS_SOA1* and *WLS_SOA2* servers listen on specific floating IPs that are failed over by Oracle WebLogic Server.

Perform the steps in the following sections to configure server migration for the managed servers.

14.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

Set up a user and tablespace for the server migration leasing table using the create tablespace leasing command.

To set up a user and tablespace for the server migration leasing table:

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the `sysdba` user and run the following command:

```
SQL> create tablespace leasing
      logging datafile 'DB_HOME/oradata/orcl/leasing.dbf'
      size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `leasing` and assign to it the `leasing` tablespace.

```
SQL> create user leasing identified by welcome1;
```

```
SQL> grant create table to leasing;
```

```
SQL> grant create session to leasing;
```

```
SQL> alter user leasing default tablespace leasing;
```

```
SQL> alter user leasing quota unlimited on LEASING;
```

3. Create the `leasing` table using the `leasing.ddl` script.
 - a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

```
WL_HOME/server/db/oracle/817
WL_HOME/server/db/oracle/920
```

- b. Connect to the database as the `leasing` user.
 - c. Run the `leasing.ddl` script in SQL*Plus.

```
SQL> @copy_location/leasing.ddl;
```

14.3 Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console

Create a multi-data source for the `leasing` table from the Oracle WebLogic Server Administration Console:

You create a data source for each of the Oracle RAC database instances during the process of setting up the multi-data source, both for these data sources and the global `leasing` multi-data source. When you create a data source:

- Make sure that this is a non-xa data source
- The names of the multi-data sources are in the format of *MultiDS-rac0*, *MultiDS-rac1*, and so on
- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11
- Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource, Emulate Two-Phase Commit**, or **One-Phase Commit** options of the **Supports Global Transactions** option), and specify a service name for your database.
- Target these data sources to the SOA cluster
- Make sure the datasources' connection pool initial capacity is set to **0**. To do this, select **Services, JDBC**, and then **Datasources**. In the Datasources screen, click the

Datasource Name, then click the **Connection Pool** tab, and enter **0** in the **Initial capacity** field.

For additional recommendations for setting up a multi-data source for Oracle RAC, see "Considerations for High Availability Oracle Database Access" in the *Oracle Fusion Middleware High Availability Guide*.

To create a multi-data source:

1. From Domain Structure window in the Oracle WebLogic Server Administration Console, expand the **Services** node, then click **Data Sources**.

The Summary of JDBC Multi Data Source page appears.

2. Click **Lock & Edit** and click **Next**.

The Create a New JDBC Multi Data Source page appears.

3. Click **Datasources**, and then **Create New Multi Data Source**.

4. Enter leasing as the Name.

5. Enter jdbc/leasing as the JNDI name.

6. Select **Failover as algorithm (default)** and click **Next**.

7. Select **SOA_Cluster** as the target and click **Next**.

8. Select **non-XA driver (the default)** and click **Next**.

9. Click **Create New Data Source**.

10. Enter *leasing-rac0* as name. Enter *jdbc/leasing-rac0* as JNDI name. Enter *oracle* as the database type. For the driver type, enter *Oracle Driver (Thin) for RAC Service-Instance connection Version 10,11*. and click **Next**.

Note: When creating the multi-datasources for the leasing table, enter names in the format of *MultiDS-rac0*, *MultiDS-rac1*, and so on.

11. Deselect **Supports Global Transactions** and click **Next**.

12. Enter the service name, database name, host port, and password for your leasing schema and click **Next**.

13. Click **Test Configuration** to verify the connection works and click **Next**.

14. Target the data source to **SOA_Cluster**.

15. Select the data source and add it to the right screen.

16. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to **SOA_Cluster**, repeating the steps for the second instance of your Oracle RAC database.

17. Add the second data source to your multi-data source.

18. Click **Activate Changes**.

14.4 Enabling Host Name Verification Certificates between SOAHOST1 and SOAHOST2 and the Administration Server

Create the appropriate certificates for host name verification between the Node Manager and the Administration Server. This procedure is described in [Section 11.3, "Enabling Host Name Verification Certificates for Node Manager in SOAHOST1 and](#)

WCPHOST1" and Section 11.5, "Enabling Host Name Verification Certificates for the Node Manager in SOAHOST2 and WCPHOST2."

14.5 Editing the Node Manager's Properties File

Edit the Node Manager properties file on the two nodes where the servers are running. The `nodemanager.properties` file is located in the following directory:

```
WL_HOME/common/nodemanager
```

Add the following properties to enable server migration to work properly:

- Interface

```
Interface=eth0
```

This property specifies the interface name for the floating IP (`eth0`, for example).

Note: Do not specify the sub interface, such as `eth0:1` or `eth0:2`. This interface is to be used without the `:0`, or `:1`. The Node Manager's scripts traverse the different `:X` enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, or `eth2`, `eth3`, `ethn`, depending on the number of interfaces configured.

- NetMask

```
NetMask=255.255.255.0
```

This property specifies the net mask for the interface for the floating IP.

- UseMACBroadcast

```
UseMACBroadcast=true
```

This property specifies whether or not to use a node's MAC address when sending ARP packets, that is, whether or not to use the `-b` flag in the `arping` command.

Verify in the output of Node Manager (the shell where the Node Manager is started) that these properties are in use. Otherwise, problems may occur during migration. The output should be similar to the following:

```
...
StateCheckInterval=500
Interface=eth0
NetMask=255.255.255.0
...
```

Note: The following steps are not required if the server properties (start properties) have been set and Node Manager can start the servers remotely.

1. If not done already, set the `StartScriptEnabled` property in the `nodemanager.properties` file to `true`. This is required to enable Node Manager to start the managed servers.

2. Start Node Manager on Node 1 and Node 2 by running the `startNodeManager.sh` script, which is located in the `WL_HOME/server/bin/` directory.

Note: When running Node Manager from a shared storage installation, multiple nodes are started using the same `nodemanager.properties` file. However, each node may require different `NetMask` or `Interface` properties. In this case, specify individual parameters on a per-node basis using environment variables. For example, to use a different interface (`eth3`) in `SOAHOSTn`, use the `Interface` environment variable as follows: `SOAHOSTn export JAVA_OPTIONS=-DInterface=eth3` and start Node Manager after the variable has been set in the shell.

14.6 Setting Environment and Superuser Privileges for the `wlsifconfig.sh` Script

Set the environment and superuser privileges for the `wlsifconfig.sh` script:

1. Ensure that the `PATH` environment variable includes the files listed in [Table 14-1](#):

Table 14-1 Required Files for the `PATH` Environment Variable

File	Directory Location
<code>wlsifconfig.sh</code>	<code>ORACLE_BASE/admin/domain_name/msserver/domain_name/bin/server_migration</code>
<code>wlscontrol.sh</code>	<code>WL_HOME/common/bin</code>
<code>nodemanager.domain</code>	<code>WL_HOME/common/nodemanager</code>

2. Grant sudo configuration for the `wlsifconfig.sh` script.
 - Configure sudo to work without a password prompt.
 - For security reasons, sudo should be restricted to the subset of commands required to run the `wlsifconfig.sh` script. For example, to set the environment and superuser privileges for the `wlsifconfig.sh` script:
 - a. Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.
 - b. Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside `/etc/sudoers` granting sudo execution privilege for `oracle` and also `ifconfig` and `arping`:

```
oracle ALL=NOPASSWD: /sbin/ifconfig, /sbin/arping
```

Note: Ask the system administrator for the sudo and system rights as appropriate to this step.

14.7 Configuring Server Migration Targets

Configure server migration targets. Configuring Cluster Migration sets the `DataSourceForAutomaticMigration` property to `true`.

To configure migration in a cluster:

1. Log into the Oracle WebLogic Server Administration Console:
`http://host:adminPort/console`

Typically, `adminPort` is 7001 by default.
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page appears.
3. Click the cluster for which you want to configure migration (**SOA_Cluster**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock & Edit**.
6. In the **Available** field, select the machine to which to allow migration and click the right arrow. In this case, select **SOAHOST1** and **SOAHOST2**.
7. Select the data source to be used for automatic migration. In this case select the leasing data source.
8. Click **Save**.
9. Click **Activate Changes**.
10. Set the Candidate Machines for Server Migration. You must perform this task for all of the managed servers as follows:
 - a. In Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
 - b. Select the server for which you want to configure migration.
 - c. Click the **Migration** tab.
 - d. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow. For **WLS_SOA1**, select **SOAHOST2**. For **WLS_SOA2**, select **SOAHOST1**.
 - e. Select **Automatic Server Migration Enabled** and click **Save**.

This enables the Node Manager to start a failed server on the target node automatically.
 - f. Click **Activate Changes**.
 - g. Restart the Administration Server and the servers for which server migration has been configured

To restart the Administration Server, use the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

Tip: Click **Customize this table** in the Summary of Servers page, move Current Machine from the Available Window to the Chosen window to view the machine on which the server is running. This will be different from the configuration if the server gets migrated automatically.

14.8 Testing Server Migration

To verify that Server Migration is working properly:

To test from Node 1:

1. Stop the WLS_SOA1 managed server.

```
kill -9 pid
```

pid specifies the process ID of the managed server. You can identify the *pid* in the node by running this command:

```
ps -ef | grep WLS_SOA1
```

2. Watch the Node Manager console: you should see a message indicating that WLS_SOA1's floating IP has been disabled.
3. Wait for the Node Manager to try a second restart of WLS_SOA1. Node Manager waits for a fence period of 30 seconds before trying this restart.
4. 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.

To test from Node 2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart WLS_SOA1 on Node 1, Node Manager on Node 2 should prompt that the floating IP for WLS_SOA1 is being brought up and that the server is being restarted in this node.
2. Access the soa-infra console in the same IP.

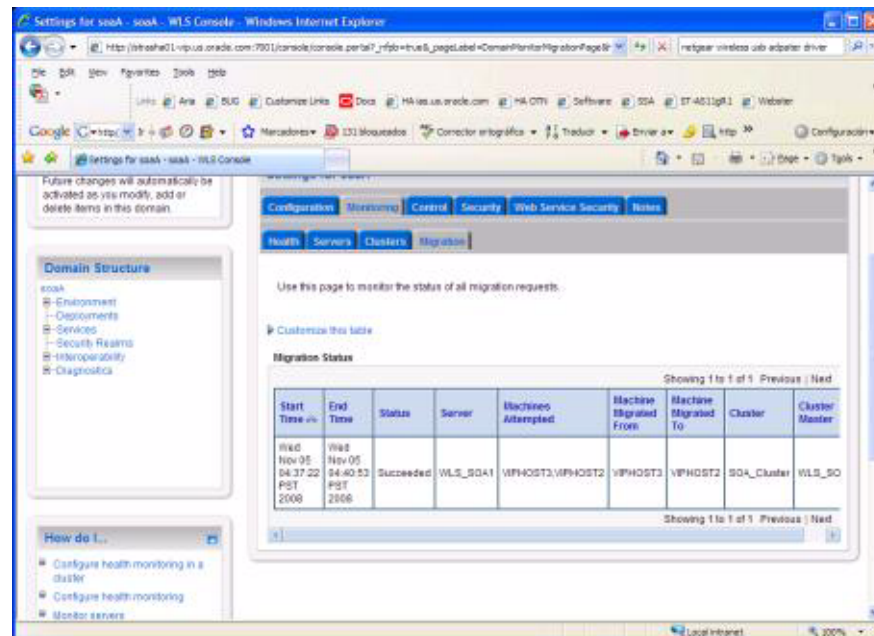
Verification From the Administration Console

You can also verify migration using the Administration Console:

1. Log into the Administration Console.
2. Click on **Domain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** subtab.

The Migration Status table provides information on the status of the migration.

Figure 14–1 Migration Status Screen in the Administration Console



Note: After a server is migrated, to fail it back to its original node/machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the managed server on the machine to which it was originally assigned.

Integrating an Enterprise Deployment with Oracle Identity Management

This chapter describes how to integrate Oracle WebCenter Portal with Oracle Identity Management. It contains the following sections:

- [Section 15.1, "Overview of Integration With Oracle Identity Management"](#)
- [Section 15.2, "Configuring the Credential Store"](#)
- [Section 15.3, "Configuring the Policy Store"](#)
- [Section 15.4, "Reassociating Credentials and Policies"](#)
- [Section 15.5, "Oracle Access Manager 10g Integration"](#)
- [Section 15.6, "Oracle Access Manager 11g Integration"](#)
- [Section 15.7, "Configuring WebCenter Portal Applications for SSO"](#)
- [Section 15.8, "Configuring WebCenter Portal and BPEL Authentication"](#)
- [Section 15.9, "Backing Up the Identity Management Configuration"](#)

15.1 Overview of Integration With Oracle Identity Management

You can integrate an Oracle Fusion Middleware enterprise deployment with Oracle Identity Manager 10g or 11g. The following sections describe how to first configure Credential and Policy stores, re-associate those credential and policy stores, and then integrate with either Oracle identity manager 10g or 11g.

[Table 15-1](#) lists the high-level steps for integrating Oracle Identity Manager 10g with an Oracle WebCenter Portal enterprise deployment.

[Table 15-2](#) lists the high-level steps for integrating Oracle Identity Manager 11g with an Oracle WebCenter enterprise deployment.

Note: When integrating with Oracle Identity Management, use the transport mode currently in use by the Oracle Identity Management servers. For example, Open, Simple or Cert.

Table 15–1 Steps for Integrating with Oracle Identity Manager 10g

Step	Description	More Information
Configure the Credential Store	Configure Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Portal Enterprise Deployment topology.	Section 15.2, "Configuring the Credential Store"
Configure the Policy Store	Configure Oracle Internet Directory LDAP as the policy store for the Oracle WebCenter Portal Enterprise Deployment topology.	Section 15.3, "Configuring the Policy Store"
Use the OAM Configuration Tool	Use the OAM Configuration Tool (oamcfg) to start a series of scripts and set up the required policies.	Section 15.5.3, "Using the OAM Configuration Tool"
Install and Configure WebGate	Install WebGate on each of the WEBHOSTn machines in order to secure the web tier.	Section 15.5.4, "Installing and Configuring WebGate"
Configure IP Validation for the Webgate	Configure the IP validation for the Webgate using Access System Console.	Section 15.5.5, "Configuring IP Validation for the Webgate"
Set Up WebLogic Authenticators	Set up the WebLogic authenticators by backing up the configuration files, setting up the OAM ID Asserter, and setting the order of providers.	Section 15.5.6, "Setting Up WebLogic Authenticators"
Configure WebCenter Portal Applications for SSO	Configure SSO system properties, the administrator role for the Spaces application, and the discussions server for SSO.	Section 15.7, "Configuring WebCenter Portal Applications for SSO"
Configure WebCenter Portal and BPEL Server Authentication	Configure WebCenter Portal and BPEL server.	Section 15.8, "Configuring WebCenter Portal and BPEL Authentication"

Table 15–2 Steps for Integrating with Oracle Identity Manager 11g

Step	Description	More Information
Configure the Credential Store	Configure Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Portal Enterprise Deployment topology.	Section 15.2, "Configuring the Credential Store"
Configure the Policy Store	Configure Oracle Internet Directory LDAP as the policy store for the Oracle WebCenter Portal Enterprise Deployment topology.	Section 15.3, "Configuring the Policy Store"
Install WebGate	Install WebGate on each of the WEBHOST machines where an HTTP Server has already been installed.	Section 15.6.3, "Installing WebGate"
Register the WebGate Agent	Register the Webgate agent using the RREG tool.	Section 15.6.4, "Registering the WebGate Agent"

Table 15–2 (Cont.) Steps for Integrating with Oracle Identity Manager 11g

Step	Description	More Information
Set Up WebLogic Authenticators	Set up the WebLogic authenticators by backing up the configuration files, setting up the OAM ID Asserter, and Setting the order of providers.	Section 15.6.5, "Setting Up the WebLogic Authenticators"
Configure WebCenter Portal Applications for SSO	Configure SSO system properties, the administrator role for the Spaces application, and the discussions server for SSO.	Section 15.7, "Configuring WebCenter Portal Applications for SSO"
Configure WebCenter Portal and BPEL Authentication	Configure WebCenter Portal and BPEL server.	Section 15.8, "Configuring WebCenter Portal and BPEL Authentication"

15.2 Configuring the Credential Store

Oracle Fusion Middleware allows using different types of credential and policy stores in a WebLogic domain. Domains can use stores based on an XML file or on different types of LDAP providers. When a domain uses an LDAP store, all policy and credential data is kept and maintained in a centralized store. However, when using XML policy stores, the changes made on Managed Servers are not propagated to the Administration Server unless they use the same domain home. The Oracle WebCenter Portal Enterprise Deployment topology uses different domain homes for the Administration Server and the Managed Server, thus Oracle requires the use of an LDAP store as policy and credential store for integrity and consistency. By default Oracle WebLogic Server domains use an XML file for the policy store. The following sections describe the steps required to change the default store to Oracle Internet Directory LDAP for credentials or policies.

Note: The backend repository for the policy store and the credential store must use the same kind of LDAP server. To preserve this coherence, note that reassociating one store implies reassociating the other one, that is, the re-association of both the credential and the policy stores is accomplished as a unit using Enterprise Manager Fusion Middleware Control or the WLST command `reassociateSecurityStore`. For more information, see [Section 15.4, "Reassociating Credentials and Policies."](#)

A credential store is a repository of security data (credentials). A credential can hold user name and password combinations, tickets, or public key certificates. Credentials are used during authentication, when principals are populated in subjects, and, further, during authorization, when determining what actions the subject can perform. In this section, steps are provided to configure Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Portal Enterprise Deployment topology. For more details on credential store configuration, refer to the "Configuring the Credential Store" chapter in the *Oracle Containers for J2EE Security Guide*.

The following section describe credential store configuration:

- [Section 15.2.1, "Creating the LDAP Authenticator"](#)
- [Section 15.2.2, "Moving the WebLogic Administrator to LDAP"](#)
- [Section 15.2.3, "Reassociating the Domain Credential Store"](#)

15.2.1 Creating the LDAP Authenticator

This section describes how to create the LDAP authenticator using the WebLogic Server Administration Console.

Prerequisites

Before you create the LDAP authenticator, back up the relevant configuration files:

```
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/config.xml
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig/jps-config.xml
ORACLE_BASE/admin/domain_name/aserver/domain_
name/config/fmwconfig/system-jazn-data.xml
```

Back up the `boot.properties` file for the Administration Server in the following directory:

```
ORACLE_BASE/admin/domain_name/aserver/domain_name/servers/AdminServer/security
```

To configure the credential store to use LDAP:

1. Log in to the WebLogic Server Console.
2. Click the **Security Realms** link on the left navigational bar.
3. Click the **myrealm** default realm entry to configure it.
4. Open the **Providers** tab within the realm.
5. Observe that there is a **DefaultAuthenticator** provider configured for the realm.
6. Click **Lock & Edit**.
7. Click the **New** button to add a new provider.
8. Enter a name for the provider such as **OIDAuthenticator** or **OVDAuthenticator** depending on whether Oracle Internet Directory or Oracle Virtual Directory will be used.
9. Select the **OracleInternetDirectoryAuthenticator** or **OracleVirtualDirectoryAuthenticator** type from the list of authenticators depending on whether Oracle Internet Directory or Oracle Virtual Directory will be used and click **OK**.
10. In the Providers screen, click the newly created Authenticator.
11. 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**; in particular, check the **DefaultAuthenticator** and set that to **SUFFICIENT**.
12. Click **Save** to save this setting.
13. Open the **Provider Specific** tab to enter the details for the LDAP server.
14. Enter the details specific to your LDAP server, as shown in the following table:

Parameter	Value	Value Description
Host	For example: oid.mycompany.com	The LDAP server's server ID.

Parameter	Value	Value Description
Port	For example: 636	The LDAP server's port number.
Principal	For example: cn=orcladmin	The LDAP user DN used to connect to the LDAP server.
Credential	NA	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	For example: cn=users, dc=us, dc= mycompany, dc=com	Specify the DN under which your Users start.
Group Base DN	For example: cn=groups, dc=us, dc= =mycompany, dc=com	Specify the DN that points to your Groups node.
Use Retrieved User Name as Principal	Checked	Must be turned on.

Click **Save** when done.

15. Click **Activate Changes** to propagate the changes.

Reorder Authenticator

Reorder the OID/OVD Authenticator and Default Authenticator and ensure that the control flag for each authenticator is set in the following order:

To set the order of the Authenticators:

1. Log in to WebLogic Console, if not already logged in.
2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, then the default realm name, and then **Providers**.
4. Reorder the OID/OVD Authenticator, and Default Authenticator by ensuring that the control flag for each authenticator is set as follows:
 - OID LDAP Authenticator (or OVD LDAP Authenticator): SUFFICIENT
 - Default Authenticator: SUFFICIENT
5. Click **OK**.
6. Click **Activate Changes** to propagate the changes.
7. Restart the Administration Server and all managed servers.

15.2.2 Moving the WebLogic Administrator to LDAP

This section provides details for provisioning a new administrator user and group for managing the Oracle Fusion Middleware WebCenter Portal WebLogic Domain. This section describes the following tasks:

- [Section 15.2.2.1, "Provisioning Admin Users and Groups in an LDAP Directory"](#)
- [Section 15.2.2.2, "Assigning the Admin Role to the Admin Group"](#)
- [Section 15.2.2.3, "Updating the boot.properties File and Restarting the System"](#)

15.2.2.1 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. Oracle does not recommend this. To avoid one WebLogic admin user having access to all the domains, the users and groups provisioned must have a unique distinguished name within the directory tree. For the WebCenter Portal enterprise deployment WebLogic domain described in this guide, the admin user and group are provisioned with the DNs below:

- Admin User DN:

```
cn=weblogic_wc,cn=Users,dc=us,dc=mycompany,dc=com
```

- Admin Group DN:

```
cn=WC_Administrators,cn=Groups,dc=us,dc=mycompany,dc=com
```

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_wc, cn=Users, dc=us, dc=mycompany, dc=com
orclsamaccountname: weblogic_wc
givenname: weblogic_wc
sn: weblogic_wc
userpassword: MyPassword1
mail: weblogic_wc
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
uid: weblogic_wc
cn: weblogic_wc
description: Admin User for the WebCenter Portal Domain
```

2. Run the `ldapadd` command located under the `ORACLE_HOME/bin` directory to provision the user in Oracle Internet Directory.

Note: The Oracle home used here is the Oracle home for the Identity Management installation where Oracle Internet Directory resides. The `ORACLE_HOME` environment variable must be set for the `ldapadd` command to succeed.

For example (the command is shown as two lines in the example below for readability purposes, but you should enter the command on a single line):

```
OIDHOST1> 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=WC_Administrators, cn=Groups, dc=us, dc=mycompany, dc=com
displayname: WC_Administrators
objectclass: top
```

```

objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_wc,cn=users,dc=us,dc=mycompany,dc=com
cn: WC_Administrators
description: Administrators Group for the SOA Domain

```

4. Run the `ldapadd` command located under the `ORACLE_HOME/bin/` directory to provision the group in Oracle Internet Directory (the command is shown as two lines in the example below for readability purposes, but you should enter the command on a single line):

```

OIDHOST1> ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D
cn="orcladmin" -w welcome1 -c -v -f admin_group.ldif

```

15.2.2.2 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.

To assign the Admin role to the Admin group:

1. Log into the WebLogic Server Administration 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 **WC_Administrators** in the **Group Argument** field and click **Add**.
7. Click **Finish** to return to the Edit Global Role page.
8. The Role Conditions table now shows the WC_Administrators Group as an entry.
9. Click **Save** to finish adding the Admin Role to the WC_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_wc user.

Note: Each SOA application has its own predefined roles and groups defined for administration and monitoring. By default, the "Administrator" group allows these operations. However, the "Administrator" group may be too broad. For example, you may not want Worklistapp Administrators to be WebLogic Server Domain Administrators where SOA is running. Therefore, you may wish to create a more specific group, such as *SOA Administrators*. In order for the different applications to allow the SOA Administrator group to administer the different systems, you must add the required application-specific roles to the SOA Administrator group. For example, for Worklistapp administration, add the *SOAAdmin* role to the SOA Administrators group. Refer to each component's specific roles for the required roles in each case.

15.2.2.3 Updating the boot.properties File and Restarting the System

The `boot.properties` file for the Administration Server should be updated with the WebLogic admin user created in Oracle Internet Directory. Follow the steps below to update the `boot.properties` file:

1. On SOAHOST1, go the following directory:

```
cd ORACLE_BASE/admin/domainName/aserver/domainName/servers/  
AdminServer/security
```

2. Rename the existing `boot.properties` file:

```
mv boot.properties boot.properties.backup
```

3. Use a text editor to create a file called `boot.properties` under the security directory. Enter the following lines in the file:

```
username=weblogic_wc  
password=welcome1
```

4. Save the file.
5. Stop the Administration Server:

```
wls:/nm/domain_name>nmKill("AdminServer")
```

6. Restart the Administration Server using the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)

15.2.3 Reassociating the Domain Credential Store

You must re-associate the credential and policy stores after configuring them. Re-associate the credential and policy stores using Enterprise Manager Fusion Middleware Control or the WLST command `reassociateSecurityStore`. See [Section 15.4, "Reassociating Credentials and Policies"](#) for detailed steps.

15.3 Configuring the Policy Store

The domain policy store is the repository of system and application-specific policies. In a given domain, there is one store that stores all policies that all applications deployed in the domain may use. This section provides the steps to configure Oracle Internet Directory LDAP as the policy store for the Oracle Fusion Middleware

WebCenter Portal Enterprise Deployment topology. This procedure consists of two parts:

- [Setting a Node in the Server Directory](#)
- [Reassociating the Domain Policy Store](#)

For more information on policy store configuration, see "OPSS Authorization and the Policy Store" chapter in the *Oracle Containers for J2EE Security Guide*.

15.3.1 Setting a Node in the Server Directory

In order to ensure the proper access to an LDAP server directory (Oracle Internet Directory) used as a policy store, you must set a node in the server directory. These steps must be completed by an Oracle Internet Directory administrator.

To create the appropriate node in an Oracle Internet Directory Server:

1. Create an LDIF file (assumed to be `jpstestnode.ldif` in this example) specifying the following DN and CN entries:

```
dn: cn=jpsroot_wc
cn: jpsroot_wc
objectclass: top
objectclass: OrclContainer
```

The distinguished name of the root node (illustrated by the string `jpsroot_wc` above) must be distinct from any other distinguished name. One root node can be shared by multiple WebLogic domains. It is not required that this node be created at the top level, as long as read and write access to the subtree is granted to the Oracle Internet Directory administrator.

2. Import this data into Oracle Internet Directory server using the command `ldapadd`, as illustrated in the following example (the command is shown as two lines in the example below for readability purposes, but you should enter the command on a single line):

```
OIDHOST1> ORACLE_HOME/bin/ldapadd -h ldap_host -p ldap_port -D
cn=orcladmin -w password -c -v -f jpstestnode.ldif
```

3. Verify that the node has been successfully inserted using the command `ldapsearch`, as illustrated in the following example (the command is shown as two lines in the example below for readability purposes, but you should enter the command on a single line):

```
OIDHOST1> ORACLE_HOME/bin/ldapsearch -h ldap_host -p ldap_port -D
cn=orcladmin -w password -b "cn=jpsroot_wc" objectclass="orclContainer"
```

4. When using Oracle internet Directory as the LDAP-Based Policy Store run the utility `oidstats.sql` in the INFRADBHOSTs to generate database statistics for optimal database performance:

```
ORACLE_HOME/bin/sqlplus
```

Enter ODS as a user name. You will be prompted for credentials for the ODS user. Inside `sqlplus`, enter the command to gather the statistics info:

```
SQLPLUS> @ORACLE_HOME/ldap/admin/oidstats.sql
```

The `oidstats.sql` utility must be run just once after the initial provisioning. For details about this utility, see the *Oracle Identity Management User Reference*.

15.3.2 Reassociating the Domain Policy Store

Reassociate the policy store by migrating policy data from a file- or LDAP-based repository to an LDAP-based repository. Re-association changes the repository preserving the integrity of the data stored. For each policy in the source policy store, re-association searches the target LDAP directory and, if it finds a match, updates the matching policy as appropriate. If none are found, it migrates the policy as is.

At any time, after a domain policy store has been instantiated, a file, or LDAP-based policy store can be reassociated into an LDAP-based policy store storing the same data. To support it, the domain has to be configured, as appropriate, to use an LDAP policy store.

For detailed steps, see [Section 15.4, "Reassociating Credentials and Policies"](#).

15.4 Reassociating Credentials and Policies

Re-associate the policy and credential store with Oracle Internet Directory using the WLST `reassociateSecurityStore` command.

To re-associate the policy and credential stores:

1. From SOAHOST1, start the `wlst` shell:

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

2. Connect to the WebLogic Administration Server using the `wlst connect` command shown below:

Syntax:

```
connect("AdminUser", "AdminUserPassword", t3://hostname:port)
```

For example:

```
connect("weblogic", "welcome1", "t3://ADMINVHN:7001")
```

3. Run the `reassociateSecurityStore` command as shown below:

Syntax:

```
reassociateSecurityStore(domain="domainName", admin="cn=orcladmin",
password="orclPassword", ldapurl="ldap://LDAPHOST:LDAPPOR", servertype="OID",
jpsroot="cn=jpsroot_wc")
```

For example:

```
wls:/WCPEDGDomain/serverConfig>reassociateSecurityStore(domain="wcpedg_domain",
admin="cn=orcladmin", password="welcome1", ldapurl="ldap://oid.mycompany.com:389",
servertype="OID", jpsroot="cn=jpsroot_wc")
```

The output for the command is shown below:

```
{servertype=OID, jpsroot=cn=jpsroot_wc_idm_idmhost1, admin=cn=orcladmin,
domain=IDMDomain, ldapurl=ldap://oid.mycompany.com:389, password=welcome1}
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
```

For more help, use `help(domainRuntime)`

```
Starting Policy Store reassociation.
LDAP server and ServiceConfigurator setup done.
```

```

Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Policy Store reassociation done.
Starting credential Store reassociation
LDAP server and ServiceConfigurator setup done.
Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Credential Store reassociation done
Jps Configuration has been changed. Please restart the server.

```

4. Restart the Administration Server after the command completes successfully.

To restart the Administration Server, use the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1"](#).

Note: For credential and policy changes to take effect, the servers in the domain must be restarted.

Cataloging Oracle Internet Directory Attributes

Index any Oracle Internet Directory attribute that is used in a search filter. The indexing is an optional procedure that enhances performance. If you have not yet indexed the attributes in this Oracle Internet Directory, use the `catalog` tool to index them.

For example, to index the `orclrolescope` attribute:

```
catalog connect="orcl" add=true attribute="orclrolescope" verbose="true"
```

You can also index multiple attribute names by listing them in a file and processing them as a batch as follows:

```

orclrolescope
orclassignedroles
orclApplicationCommonName
orclAppFullName
orclCSFAlias
orclCSFKey
orclCSFName
orclCSFDBUrl
orclCSFDBPort
orclCSFCredentialType
orclCSFExpiryTime
modifytimestamp
createtimestamp
orcljpsassignee

```

For more information about indexing OID attributes, see Tasks and Examples for `catalog` in the *Oracle Fusion Middleware Reference for Oracle Identity Management*.

15.5 Oracle Access Manager 10g Integration

This section describes how to set up Oracle Access Manager 10g as the single sign-on solution for the Oracle WebCenter Portal Enterprise Deployment topology.

Note: If you are integrating with Oracle Access Manager 11g, skip this section, follow steps in [Section 15.6, "Oracle Access Manager 11g Integration,"](#) and then proceed to [Section 15.7, "Configuring WebCenter Portal Applications for SSO,"](#) and continue on with the rest of this chapter.

This section contains the following subsections:

- [Section 15.5.1, "Overview of Oracle Access Manager Integration"](#)
- [Section 15.5.2, "Prerequisites for Oracle Access Manager"](#)
- [Section 15.5.3, "Using the OAM Configuration Tool"](#)
- [Section 15.5.4, "Installing and Configuring WebGate"](#)
- [Section 15.5.5, "Configuring IP Validation for the Webgate"](#)
- [Section 15.5.6, "Setting Up WebLogic Authenticators"](#)
- [Section 15.5.7, "Configuring Virtual Hosts for OAM 10g"](#)

15.5.1 Overview of Oracle Access Manager Integration

Oracle Access Manager (OAM) is the recommended single sign-on solution for Oracle Fusion Middleware 11g Release 1. For more information on installing and configuring an OAM installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This chapter explains the procedure for configuring the WebCenter Portal installation with an existing OAM installation and the underlying directory service. Oracle recommends using either Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD) or both of these directory services.

Note: The WebCenter Portal Enterprise Deployment topology described in this book uses a Single Sign-On configuration where both the WebCenter Portal System and the Single Sign-On System are in the same network domain (mycompany.com) For a multi-domain configuration, please refer to the required configuration steps in "Configuring Single Sign-On," of the *Oracle Access Manager Access Administration Guide*.

15.5.2 Prerequisites for Oracle Access Manager

The setup for Oracle Access Manager (OAM) assumes an existing OAM installation complete with Access Managers and a policy protecting the Policy Manager. For more information on installing and configuring an OAM installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This setup includes a directory service such as Oracle Internet Directory (OID) either as a stand-alone or as part of an Oracle Virtual Directory (OVD) configuration. This chapter will provide the necessary steps for configuring your WebCenter Portal installation with either OID or OVD.

In addition, the OAM installation should have its own Web server configured with WebGate. This section also provides the steps for using the OAM Web server as a delegated authentication server.

15.5.3 Using the OAM Configuration Tool

The OAM Configuration Tool (oamcfg) starts a series of scripts and setup the required policies. It requires various parameters as inputs. Specifically, it creates the following:

1. A Form Authentication scheme in OAM
2. Policies to enable authentication in WebLogic Server
3. An WebGate entry in OAM to enable Oracle HTTP Server WebGates (from your web tier) to protect your configured application
4. A Host Identifier, depending on the scenario chosen (a default host identifier would be used, if not provided)
5. Policies to protect and unprotect application specific URLs.

This section covers the following topics:

- [Section 15.5.3.1, "Prerequisites for Running the OAM Configuration Tool"](#)
- [Section 15.5.3.2, "Running the OAM Configuration Tool"](#)
- [Section 15.5.3.3, "Updating the REST Policies"](#)
- [Section 15.5.3.4, "Creating an Exclusion Policy for Oracle SES and Portlets"](#)
- [Section 15.5.3.5, "Verifying Successful Creation of the Policy Domain and AccessGate"](#)
- [Section 15.5.3.6, "Updating the Host Identifier"](#)
- [Section 15.5.3.7, "Updating the WebGate Profile"](#)
- [Section 15.5.3.8, "Adding Additional Access Servers"](#)
- [Section 15.5.3.9, "Configuring Delegated Form Authentication"](#)

15.5.3.1 Prerequisites for Running the OAM Configuration Tool

Review the following prerequisites before running the OAM Configuration Tool:

- **Password:** Create a secure password. This will be used as the password for the WebGate installation created later.
- **LDAP Host:** Have the host name of the Directory Server or Load Balancer address available in the case of a high availability or enterprise deployment configuration.
- **LDAP Port:** Have the port of the Directory Server available.
- **LDAP USER DN:** Have the DN of the LDAP admin user available. This is a value such as "cn=orcladmin."
- **LDAP password:** Have the password of the LDAP admin user available.
- **oam_aa_host:** Have the host name of an Oracle Access Manager available.
- **oam_aa_port:** Have the port of the Oracle Access Manager available.

15.5.3.2 Running the OAM Configuration Tool

You can find the OAM Configuration Tool at the following location:

`ORACLE_COMMON_HOME/modules/oracle.oamprovider_11.1.1`

`ORACLE_COMMON_HOME` depends on the machine on which you are running the configuration tool. The tool can be run from any machine with the required installation files. The procedure described in this section runs the tool from `SOAHOST1`.

The OAM Configuration Tool should be run as follows (all on a single command line):

```
MW_HOME/jrockit_160_<version>/bin/java -jar oamcfgtool.jar mode=CREATE
app_domain="WebCenter_EDG"
protected_uris="$URI_LIST"
public_uris="$PUBLIC_URI_LIST"
app_agent_password=<Password_to_be_provisioned_for_App_Agent>
ldap_host=OID.MYCOMPANY.COM
ldap_port=389
ldap_userdn="cn=orcladmin"
ldap_userpassword=<Password_of_LDAP_Admin_User>
oam_aaa_host=OAMHOST1
oam_aaa_port=OAMPOR1
```

The \$URI_LIST and \$PUBLIC_URI_LIST variables in the above command depend on the topology:

- **WebCenter Portal, WebCenter Content, and Inbound Refinery in the domain:**

```
$URI_LIST="
/webcenter/adfAuthentication,
/integration/worklistapp,
/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow,
/workflow/WebCenterWorklistDetail/faces/adf.task-flow,
/workflow/sdpmessagingsca-ui-worklist,
/soa-infra,
/rss/rssservlet,
/owc_discussion/login!withRedirect.jspa,
/owc_discussions/login!default.jspa,
/owc_discussions/login.jspa,
/owc_discussions/admin,
/rest/api/resourceIndex,
/rest/api/spaces,
/rest/api/discussions,
/rest/api/tags,
/rest/api/taggeditems,
/rest/api/activities,
/rest/api/activitygraph,
/rest/api/feedback,
/rest/api/people,
/rest/api/messageBoards,
/rest/api/searchresults,
/activitygraph-engines,
/wcps/api,
/pagelets/admin,
/pagelets/authenticateWithApplicationServer,
/services-producer/adfAuthentication,
/rsscrawl,
/sesUserAuth,
/services-producer/portlets,
/wsrp-tools/portlets
/em,
/console,
/adfAuthentication,
/ibr/adfAuthentication"

$PUBLIC_URI_LIST="
/webcenter,
```

```

/owc_discussions,
/rss,
/rest/api/cmisis,
/pagelets,
/services-producer,
/wsrp-tools,
/workflow,
/cs,
/ibr,
/idcnativews,
/"

```

- **WebCenter Portal, WebCenter Content, Inbound Refinery, and SOA in the domain:**

```

$URI_LIST="
/webcenter/adfAuthentication,
/integration/worklistapp,
/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow,
/workflow/WebCenterWorklistDetail/faces/adf.task-flow,
/workflow/sdpmessagingsca-ui-worklist,
/rss/rssservlet,
/owc_discussions/login!withRedirect.jspa,
/owc_discussions/login!default.jspa,
/owc_discussions/login.jspa,
/owc_discussions/admin,
/rest/api/resourceIndex,/rest/api/spaces,/rest/api/discussions,
/rest/api/tags,/rest/api/taggeditems,/rest/api/activities,
/rest/api/activitygraph,/rest/api/feedback,/rest/api/people,
/rest/api/messageBoards,/rest/api/searchresults,
/activitygraph-engines,
/wcps/api,
/pagelets/admin,
/pagelets/authenticateWithApplicationServer,
/services-producer/adfAuthentication
/rsscrawl,
/sesUserAuth,
/services-producer/portlets,
/wsrp-tools/portlets,
/em,/console,/DefaultToDoTaskFlow,
/sdpmessaging/userprefs-ui,
/adfAuthentication,
/ibr/adfAuthentication,
/soa-infra,/soa/composer,/soa-infra/deployer,/soa-infra/events/edn-db-log,/soa-infra/cluster/info,/inspection.wsil"

$PUBLIC_URI_LIST="
/webcenter,
/owc_discussions,
/rss,
/workflow,
/rest/api/cmisis,
/pagelets,
/services-producer,
/wsrp-tools,
/cs,
/ibr,

```

```

/idcnativevs,
/,
/soa-infra/services/.../*,/soa-infra/directWSDL,/soa-infra/dire
ctWSDL/.../*,/ucs/messaging/webservice,/ucs/messaging/webservic
e/.../*"

```

Note:

- If SOA is added to the domain later or other additional URLs need to be protected, the OAM configuration tool should be executed again using the same `app_domain` and including *all* the URLs that would be protected (not just the new ones).
 - WebCenter Portal, SOA, and WebCenter Content each provide `.conf` file that lists their public and protected URI requirements. Instead of specifying public and protect URIs using the `protected_uris=` and `public_uris=` syntax as shown, you can reference each file in turn using the syntax `uris_file=`. For more information and instructions, see "Configuring the WebCenter Portal Policy Domain" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.
-
-

If your command ran successfully, you should see the following output:

```

Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation
Operation Summary:
Policy Domain: WebCenter_EDG
Host Identifier: WebCenter_EDG
Access Gate ID: WebCenter_EDG_AG

```

15.5.3.3 Updating the REST Policies

To update the REST end points to use basic authentication:

1. Log in to the Oracle Access Manager console at `http://OAM_HOST:OAM_ADMINSERVER_PORT/oamconsole`.
2. Locate the policy domain that you created and verified in the previous steps and open the **Policies** tab.

You should see two policies already created **Protected_JSessionId_Policy** and **Default Public Policy**.

3. Create another policy called **WebCenterRESTPolicy**, using the values shown below:

Description: This policy protects REST protected URIs using BASIC authentication scheme required for functioning with the WebCenter Outlook plug-in or iPhone integration.

Resource Type: http

Operation(s): GET, POST

Resource: Select all resources starting with `/rest` except for `/rest/cmis/repository`.

`/rest/api/resourceIndex`

```

/rest/api/spaces
/rest/api/discussions
/rest/api/tags
/rest/api/taggeditems
/rest/api/activities
/rest/api/activitygraph
/rest/api/feedback
/rest/api/people
/rest/api/messageBoards
/rest/api/searchresults

```

Host Identifier: Same as the one used for the resources.

4. Click **Save**.
5. In the newly created policy, navigate to **Authentication Rule** and add a new rule using the authentication scheme `OraDefaultBasicAuthNScheme`.
6. Open the **Policies** tab and make sure that the policies are in the order shown below:

```

WebCenterRESTPolicy
Protected_JSessionId_Policy
Default Public Policy

```

15.5.3.4 Creating an Exclusion Policy for Oracle SES and Portlets

To create an exclusion policy for Oracle SES (Secure Enterprise Search) and portlets:

1. Log in to the Oracle Access Manager console at:
http://OAM_HOST:OAM_ADMINSERVER_PORT/oamconsole
2. Check that `OraDefaultExclusionAuthNScheme` is available in your OAM 10g installation. If it does not exist, create the `OraDefaultExclusionAuthNScheme` as shown below:
 - a. Click **Authentication Management**.
 - b. Click **Add**.
 - c. Specify `OraDefaultExclusionAuthNScheme` in the **Name** field.
 - d. Enter `To exclude resources from being protected by OAM` in the **Description** field.
 - e. Enter `0` in the **Level** field.
 - f. Specify `None` in the **Challenge Method** field.
 - g. Add `unprotected:true` to the **Challenge Parameter** field.
 - h. Click **Save**.
 - i. Open the **Plugins** tab for this authentication scheme and click **Modify**.
 - j. Select `credential_mapping` from the drop down list.
 - k. Specify a value as:

```

obMappingBase="dc=us,dc=oracle,dc=com",obMappingFilter="(uid=OblixAnonymous)"

```

Make sure that this value matches the corresponding field for the `OraDefaultAnonAuthNScheme`.

column URL prefixes, the URIs you specified during the creation of this domain appear.

4. Click the link to the policy domain you just created.

This link takes you to the General area of this domain.

5. Click the **Resources** tab.

The URIs you specified appear. You can also click other tabs to view other settings.

To verify the AccessGate configuration:

1. Click the **Access System Console** link on the top right hand side.

This acts like a toggle; after you click it, it becomes the **Policy Manager** link.

2. Click the **Access System Configuration** tab.

3. Click the **AccessGate Configuration** link on the left panel.

4. Enter **WebCenter_EDG** as the search criterion (or any other substring you may have used as the `app_domain` name in [Section 15.5.3.2, "Running the OAM Configuration Tool"](#)), and click **Go**.

5. Once the AccessGate for the domain you just created appears (this will have the suffix `_AG` (for example, `WebCenter_EDG_AG`), click it, and the details of the AccessGate which you just created appear.

15.5.3.6 Updating the Host Identifier

The OAM Configuration Tool uses the value of the `app_domain` parameter (for example, `WebCenter_EDG`) to create a host identifier for the policy domain. This host identifier must be updated with all the host name 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. Log in to the Access System Console using the following URL:

```
http://OAMADMINHOST:port/access/oblix
```

where `OAMADMINHOST` 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.

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 `WebCenter_EDG`.
7. On the Host Identifier Details page, click **Modify**.
8. Add the **Preferred HTTP Host** value used in the Access System Configuration. The following is a list of all the possible host name variations using SSO/WebGate:
 - `webhost1.mydomain.com:7777`
 - `webhost2.mydomain.com:7777`

- wcpghost1:9000
 - wcpghost2:9000
 - wcpghost1:9001
 - wcpghost2:9001
 - wcpghost1:9002
 - wcpghost2:9002
 - wcpghost1:9003
 - wcpghost2:9003
 -
 - admin.mycompany.com
 - adminvhn.mycompany.com:7001
 - soahost1vhn1:8001
 - soahost2vhn1:8001
 - soahost1vhn1:8010
 - soahost2vhn1:8010
 - adminvhn:7001
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.

15.5.3.7 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. Log in to the Access System Console using the following URL:
`http://OAMADMINHOST:port/access/oblix`

where `OAMADMINHOST` 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.
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 **Access System Configuration**, and then click the **Access Gate Configuration** link on the left pane 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: WebCenter_EDG_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:80`.
 - **Primary HTTP Cookie Domain:** Update the Primary HTTP Cookie Domain with the Domain suffix of the host identifier, for example: `mycompany.com`
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.

15.5.3.8 Adding Additional Access Servers

To assign an Access Server to the WebGate:

1. Log in as Administrator to Oracle Access Manager using the following URL:

`http://OAMADMINHOST:port/access/oblix`

where *OAMADMINHOST* 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.

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 (**WebCenter_EDG_AG**).
3. On the **Details** for AccessGate page, click **List Access Servers**.
4. A page appears showing the primary or secondary Access Servers currently configured for this WebGate.
Click **Add**.
5. On the Add a New Access Server page, select an Access Server from the **Select Server** list, specify **Primary Server**, and increase the **Number of Connections** for the WebGate. For example, increment the number of connections from 1 to 2.

Note: The Number of Connections must be equal or greater than the total number of Access Servers. Each time you add an Access Server you must increment the number of connections by 1.

Click the **Add** button to complete the association.

6. A page appears, showing the association of the Access Server with the WebGate. Click the link to display a summary and print this page for later use.

7. Repeat steps 3 through 6 to associate all the Access Servers you have defined to the WebGate.

15.5.3.9 Configuring Delegated Form Authentication

To configure the form authentication to redirect to the WebGate that was installed with the OAM installation:

1. Open the Access System Console.
2. In the Access System Configuration screen, select **Authentication Management** from the left-hand bar.
3. Select **OraDefaultFormAuthNScheme**.
4. Click **Modify**.
5. In the **Challenge Redirect** field, enter the host and port of the Oracle HTTP Server for the IDM installation; for example: `http://sso.mycompany.com:7777`.

A WebGate should already be installed in the IDM installation. Refer to, "Installing and Configuring WebGate" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for details.

15.5.4 Installing and Configuring WebGate

Install WebGate on each of the WEBHOST n machines in order to secure the web tier:

1. Launch the WebGate installer (see [Section 2.4, "Identifying the Software Components to Install"](#) for information on where to obtain it) using the following command:

```
./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate -gui
```

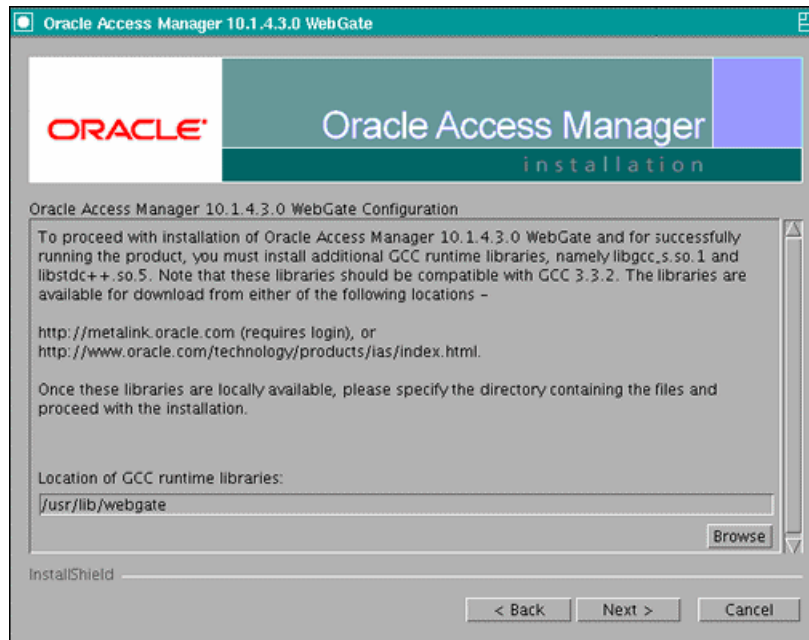
2. The Welcome screen displays. Click **Next**.
3. In the Customer Information screen ([Figure 15-1](#)), enter the user name and user group that the web server is running as. Click **Next** to continue.

Figure 15–1 Customer Information Screen

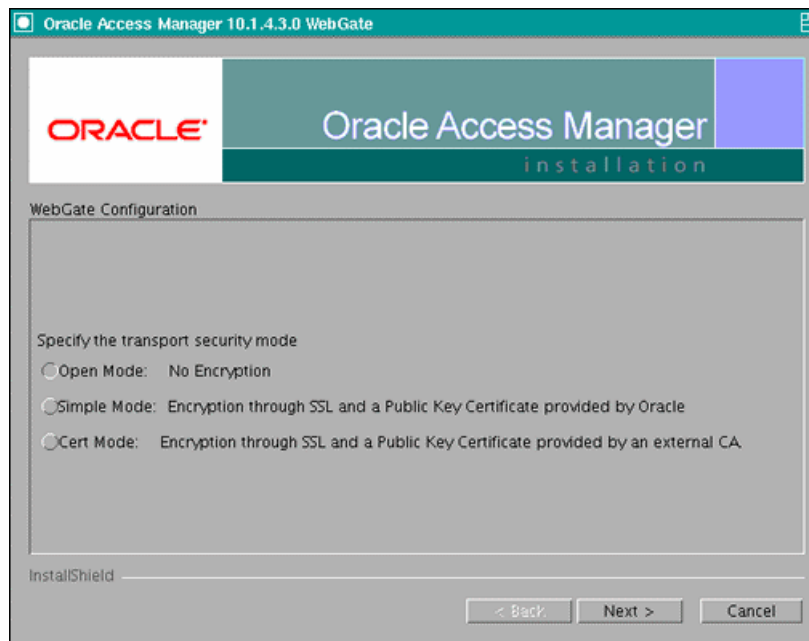
4. In the installation target screen (Figure 15–2), specify the directory where WebGate should be installed. Click **Next** to continue.

Figure 15–2 Installation Target Screen

5. In the installation summary screen, click **Next**.
6. Download the required GCC runtime libraries for WebGate as instructed in the WebGate configuration screen (Figure 15–3), and use **Browse** to point to their location on the local computer. Click **Next** to continue.

Figure 15–3 Runtime Libraries Screen

7. The installer now creates the required artifacts. After that is completed, click **Next** to continue.
8. In the transport security mode screen (Figure 15–4), select "Open Mode: No Encryption" and click **Next** to continue.

Figure 15–4 Transport Security Mode Screen

9. In the WebGate configuration screen, provide the details of the Access Server that will be used. You must provide the following information:
 - **WebGate ID**, as provided when the OAM configuration tool was executed

- **Password for WebGate**
- **Access Server ID**, as reported by the OAM Access Server configuration
- **Access Server host name**, as reported by the OAM Access Server configuration
- **Access Server port number**, as reported by the OAM Access Server configuration

Note: The Access Server ID, host name, and port are all required.

You can obtain these details from your Oracle Access Manager administrator. Click **Next** to continue.

Figure 15–5 Access Server Configuration Screen

10. In the Configure Web Server screen, click **Yes** to automatically update the web server. Click **Next** to continue.

11. In the next Configure Web Server screen, specify the full path of the directory containing the `httpd.conf` file. This file is located in the following directory:

`ORACLE_BASE/admin/OHS_Instance/config/OHS/OHS_ComponentName`

For example:

`ORACLE_BASE/admin/ohs_instance2/config/OHS/ohs2/httpd.conf`

Click **Next** to continue.

12. In the next Configure Web Server page, a message informs you that the Web server configuration has been modified for WebGate. Click **Yes** to confirm.

13. Stop and start your Web server for the configuration updates to take effect. Click **Next** to continue.

14. In the next Configure Web Server screen, the following message is displayed: "If the web server is set up in SSL mode, then the 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** to continue.
15. In 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. Choose **No** and click **Next** to continue.
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** to continue.
17. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next** to continue.
18. A message appears (along with the details of the installation) informing you that the installation was successful.

15.5.5 Configuring IP Validation for the Webgate

IP Validation determines if a client's IP address is the same as the IP address stored in the `ObSSOCookie` generated for single sign-on. IP Validation can cause issues in systems using load balancer devices configured to perform IP termination, or when the authenticating webgate is front-ended by a different load balancer from the one front-ending the enterprise deployment.

To configure your load balancer so that it is not validated in these cases:

1. Navigate to the Access System Console using the following URL:

```
http://OAMADMINHOST:port/access/oblix
```

Where the `OAMADMINHOST` refers to the host where the WebPass Oracle HTTP Server instance is running, and `port` refers to the HTTP port of the Oracle HTTP Server instance.

2. On the Access System main page, click the **Access System Console** link, and then log in as an administrator.
3. On the Access System Console main page, click **Access System Configuration**, and then click the **Access Gate Configuration** link on the left pane 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 Oracle Access Manager configuration tool.
6. Click **Modify** at the bottom of the page.
7. In the `IPValidationException` field, enter the address of the load balancer used to front-end the deployment.
8. Click **Save** at the bottom of the page.

15.5.6 Setting Up WebLogic Authenticators

This section describes how to set up WebLogic Authenticators.

Prerequisite

If you have not already created the LDAP authenticator, do it before continuing with this section. To set up the LDAP authenticator, follow the steps in [Section 15.2.1, "Creating the LDAP Authenticator."](#)

This section includes the following topics:

- [Section 15.5.6.1, "Back Up Configuration Files"](#)
- [Section 15.5.6.2, "Setting Up the OAM ID Asserter"](#)
- [Section 15.5.6.3, "Setting the Order of Providers"](#)

15.5.6.1 Back Up Configuration Files

To be safe, first back up the relevant configuration files (stored under WebCenter Portal's Administration Server directory):

```
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/config.xml
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig/jps-config.xml
ORACLE_BASE/admin/domain_name/aserver/domain_
name/config/fmwconfig/system-jazn-data.xml
```

Also back up the `boot.properties` file for the Administration Server.

15.5.6.2 Setting Up the OAM ID Asserter

Set up the OAM ID Asserter using the WebLogic Server Administration Console.

To set up the OAM ID Asserter:

1. Log in as an administrator to WebLogic Server Administration Console.
2. Navigate to the following location:


```
SecurityRealms\Default_Realm_Name\Providers
```
3. Click **New** and Select **OAM Identity Asserter** from the dropdown menu.
4. Name the asserter (for example, **OAM ID Asserter**) and click **Save**.
5. Click the newly added asserter to see the configuration screen for OAM Identity Asserter.
6. Set the control flag to **REQUIRED** and click **Save**.
7. Check that **OAM_REMOTE_USER** and **ObSSOCookie** is set for **Chosen Types**.
8. Save the settings.

15.5.6.3 Setting the Order of Providers

To set the order of the providers:

1. Log in as an administrator to Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, then the default realm name, and then **Providers**.
4. Reorder the OAM Identity Asserter, OID/OVD Authenticator, and Default Authenticator by ensuring that the control flag for each authenticator is set as follows:
 - OAM Identity Asserter: **REQUIRED**
 - OID LDAP Authenticator (or OVD LDAP Authenticator): **SUFFICIENT**

- Default Authenticator: SUFFICIENT
5. Click **OK**.
 6. Click **Activate Changes** to propagate the changes.
 7. Restart the Administration Server and all managed servers.

15.5.7 Configuring Virtual Hosts for OAM 10g

To configure OAM 10g for virtual hosts, bypass single sign-on for applications that only support BASIC authorization or do not require single sign-on.

For more information, see "Configuring SSO with Virtual Hosts" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal* and "Associating a WebGate with Particular Virtual Hosts, Directories, or Files" in *Oracle Access Manager Access Administration Guide for 10g*.

1. Locate and comment out the following configuration in `httpd.conf`:

```
#<LocationMatch "/*">  
#AuthType Oblix  
#require valid-user  
#</LocationMatch>
```

This entry causes the WebGate to intercept all requests and process them.

2. Edit the virtual host configuration section as follows:

```
NameVirtualHost *:7777  
  
<VirtualHost *:7777>  
  ServerName https://wcp.mycompany.com:443  
  <LocationMatch "/*">  
    AuthType Oblix  
    require valid-user  
  </LocationMatch>  
</VirtualHost>  
  
<VirtualHost *:7777>  
  ServerName admin.mycompany.com:80  
  <LocationMatch "/*">  
    AuthType Oblix  
    require valid-user  
  </LocationMatch>  
</VirtualHost>  
  
<VirtualHost *:7777>  
  ServerName wcpinternal.mycompany.com:80  
  <LocationMatch "/*">  
    AuthType Oblix  
    require valid-user  
  </LocationMatch>  
</VirtualHost>  
  
#Virtual host for SharePoint access  
<VirtualHost *:7777>  
  ServerName wcp-spaces.mycompany.com  
  ServerAdmin you@your.address  
  RewriteEngine On  
  RewriteOptions inherit
```



```

#SharePoint entry point
<Location />
    WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Spaces Application
<Location /webcenter>
    Deny from all
</Location>

<Location /webcenterhelp>
    Deny from all
</Location>

<Location /rss>
    Deny from all
</Location>

<Location /rest>
    Deny from all
</Location>

</VirtualHost>

```

3. Restart Oracle HTTP Server.

15.6 Oracle Access Manager 11g Integration

This section describes how to set up Oracle Access Manager 11g as the single sign-on solution for the Oracle WebCenter Portal Enterprise Deployment topology.

This section contains the following sections:

- [Section 15.6.1, "Overview of Oracle Access Manager Integration"](#)
- [Section 15.6.2, "Prerequisites for Oracle Access Manager"](#)
- [Section 15.6.3, "Installing WebGate"](#)
- [Section 15.6.4, "Registering the WebGate Agent"](#)
- [Section 15.6.5, "Setting Up the WebLogic Authenticators"](#)
- [Section 15.6.6, "Configuring Virtual Hosts for OAM11g"](#)

15.6.1 Overview of Oracle Access Manager Integration

Oracle Access Manager (OAM) is the recommended single sign-on solution for Oracle Fusion Middleware 11g Release 1. For more information on installing and configuring an OAM installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This section explains the procedure for configuring the WebCenter Portal installation with an existing OAM 11g installation and the underlying directory service. Oracle recommends using either Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), or both of these directory services.

Note: The WebCenter Portal topology described in this guide uses a Single Sign-On configuration where both the WebCenter Portal System and the Single Sign-On System are in the same network domain (mycompany.com). For a multi-domain configuration, please refer to the required configuration steps in "Configuring Single Sign-On," of the *Oracle Access Manager Access Administration Guide*.

15.6.2 Prerequisites for Oracle Access Manager

Oracle Access Manager (OAM) is the recommended single sign-on solution for Oracle Fusion Middleware 11g Release 1. For more information on installing and configuring an OAM installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This section explains the procedure for configuring the WebCenter Portal installation with an existing OAM 11g installation and the underlying directory service. Oracle recommends using either Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), or both of these directory services.

Note: The WebCenter Portal topology described in this guide uses a Single Sign-On configuration where both the WebCenter Portal System and the Single Sign-On System are in the same network domain (mycompany.com). For a multi-domain configuration, refer to the required configuration steps in "Configuring Single Sign-On," of the *Oracle Access Manager Access Administration Guide*.

15.6.3 Installing WebGate

This section describes how to install WebGate on each of the WEBHOST machines where an HTTP Server has already been installed.

- [Prerequisite for Installing GCC Libraries](#)
- [Installing WebGate](#)
- [Post-Installation Steps](#)

15.6.3.1 Prerequisite for Installing GCC Libraries

Before installing WebGate, download and install third-party GCC libraries on your machine. You can download the appropriate GCC library from the following third-party Web site:

<http://gcc.gnu.org/>

For Linux 32-bit the required libraries are libgcc_s.so.1 and libstdc++.so.5 version 3.3.2. [Table 15-3](#) lists the versions of GCC third-party libraries for Linux and Solaris.

Table 15-3 Versions of GCC Third-Party Libraries for Linux and Solaris

Operating System	Architecture	GCC Libraries	Required Library Version
Linux 32-bit	x86	libgcc_s.so.1	3.3.2
		libstdc++.so.5	
Linux 64-bit	x64	libgcc_s.so.1	3.4.6
		libstdc++.so.6	
Solaris 64-bit	SPARC	libgcc_s.so.1	3.3.2
		libstdc++.so.5	

15.6.3.2 Installing WebGate

This section describes the procedures for installing WebGate.

The Installer program for Oracle HTTP Server 11g Webgate for Oracle Access Manager is included in the `webgate.zip` file.

To install WebGate:

1. Extract the contents of the `webgate.zip` file to a directory.
By default, this directory is named `webgate`.
2. Move to the `Disk1` directory under the `webgate` directory.
3. Set the `MW_HOME` environment variable to the Middleware Home for the web tier:

```
export MW_HOME=ORACLE_BASE/product/fmw/web
```

4. Start the installer using the following command:

```
$ ./runInstaller -jreLoc MW_HOME/jdk
```

Note: When you install Oracle HTTP Server, the `jdk` directory is created under the `WebTier_Home` directory. You must enter the absolute path of the JRE folder located in this JDK when launching the installer.

After the installer starts, the Welcome screen appears.

5. In the Welcome screen, click **Next**.
6. In the Prerequisite Checks screen, click **Next**.
7. In the Specify Installation Location screen, specify the Oracle Middleware Home and Oracle Home locations.
 - `ORACLE_BASE/product/fmw`
 - `Oracle_OAMWebGate1` (leave the default name)

Note: The Middleware Home contains an Oracle Home for Oracle web tier. The default name is `Oracle_OAMWebGate1` for this Oracle home directory, which will be created under the Middleware Home.

Click **Next**.

8. In the Specify GCC Library screen, specify the directory that contains the GCC libraries, and click **Next**.
9. In the Installation Summary screen, verify the information on this screen and click **Install** to begin the installation.
10. In the Installation Progress screen, you may be prompted to run the `ORACLE_HOME/oracleRoot.sh` script to set up the proper file and directory permissions.
Click **Next** to continue.
11. In the Installation Complete screen, click **Finish** to exit the installer.

15.6.3.3 Post-Installation Steps

Complete the following procedure after installing Oracle HTTP Server 11g Webgate for Oracle Access Manager:

1. Move to the following directory under your Oracle Home for Webgate:

```
$ cd Webgate_Oracle_Home/webgate/ohs/tools/deployWebGate
```

Webgate_Oracle_Home is the directory where you have installed Oracle HTTP Server Webgate and created as the Oracle Home for Webgate, as in the following example:

```
MW_HOME/Oracle_OAMWebGate1
```

2. On the command line, run the following command to copy the required bits of agent from the *Webgate_Oracle_Home* directory to the Webgate Instance location:

```
$ ./deployWebGateInstance.sh -w ORACLE_BASE/admin/webN/config/OHS/ohsN  
-oh Webgate_Oracle_Home
```

The *ORACLE_BASE*/admin/webN/config/OHS/ohsN directory is the Instance Home of an Oracle HTTP Server (where *N* is a sequential number for your installation; for example, 1 for WEBHOST1 or 2 for WEBHOST2).

Note: an Instance Home for Oracle HTTP Server is created after you configure Oracle HTTP Server.

3. Run the following command to ensure that the LD_LIBRARY_PATH variable contains *Oracle_Home_for_Oracle_HTTP_Server/lib*:

```
$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:ORACLE_BASE/product/fmw/webN/lib
```

Note: *Oracle_Home_for_Oracle_HTTP_Server* is *MW_HOME* (web tier):

```
ORACLE_BASE/product/fmw/webN
```

Where *N* is a sequential number for your installation; for example, 1 for WEBHOST1, 2 for WEBHOST2, and so on.

4. From your present working directory, move up one directory level:

```
$ cd Webgate_Oracle_Home/webgate/ohs/tools/setup/InstallTools
```

5. On the command line, run the following command to copy the apache_ webgate.template from the *Webgate_Oracle_Home* directory to the Webgate Instance location (renamed to webgate.conf) and update the httpd.conf file to add one line to include the name of webgate.conf:

```
$ ./EditHttpConf -w ORACLE_BASE/admin/webN/config/OHS/ohsN [-oh Webgate_Oracle_Home] [-o output_file]
```

Note: The -oh *WebGate_Oracle_Home* and -o *output_file* parameters are optional.

Where *WebGate_Oracle_Home* is the directory where you have installed Oracle HTTP Server Webgate for Oracle Access Manager and created as the Oracle Home for Webgate, as in the following example:

```
MW_HOME/Oracle_OAMWebGate1
```

The *ORACLE_BASE/admin/webN/config/OHS/ohsN* directory is the instance home of Oracle HTTP Server, where *N* is a sequential number for your installation; for example, 1 for WEBHOST1 or 2 for WEBHOST2.

The *output_file* is the name of the temporary output file used by the tool, as in the following example:

```
Edithttpconf.log
```

15.6.4 Registering the WebGate Agent

This section describes the procedures for registering the WebGate Agent.

- [The RREG Tool](#)
- [Updating the OAM11gRequest file](#)
- [Running the oamreg Tool](#)
- [Copying Access files to WEBHOSTs](#)
- [Updating REST Policies](#)

15.6.4.1 The RREG Tool

The RREG tool is part of the OAM 11g installation. If it is not already available, extract it using the following procedure:

1. After installing and configuring Oracle Access Manager, navigate to the following location:

```
IDM_Home/oam/server/rreg/client
```

2. On the command line, untar the RREG.tar.gz file using gunzip, as in the following example:

```
gunzip RREG.tar.gz
```

```
tar -xvf RREG.tar
```

You can find the tool that is used to register the agent in the following location:

```
RREG_Home/bin/oamreg.sh
```

RREG_Home is the directory to which you extracted the contents of RREG.tar.gz/rreg.

Set the following environment variables in the `oamreg.sh` or `oamreg.bat` script:

- `OAM_REG_HOME` - Set this variable to the absolute path to the directory where you extracted the contents of RREG.tar/rreg.
- `JDK_HOME` - Set this variable to the absolute path to the directory where Java/JDK is installed on your machine.

15.6.4.2 Updating the OAM11gRequest file

In the `RREG_Home/input` directory there are template files named `OAM11gRequest.xml`. Copy and edit this file to create the policies for the WebCenter Portal installation.

1. Open the template `OAM11gRequest.xml` file available in `RREG_Home/input`.
2. Copy policies required for the WebCenter Portal enterprise deployment provided in [Example 15-1](#).
3. Replace the following values:
 - `$$webtierhost$$`, `$$oamadminserverport$$`, and `$$oamhost$$` with the hostnames in your installation
 - `ipvalidationExceptions` value with the IP address of the Load Balancer

Note: -This Guide describes the validation field entry in request files for Oracle Access Manager 11g (11.1.1.2) and later. The validation exception list is defined differently in earlier versions of Oracle Access Manager 11g. For earlier versions, instead of using the `<ValList>` entry as shown in the preceding text, use this syntax after the `</publicResourcesList>` entry:

```
<userDefinedParameters>
  <userDefinedParam>
    <name>ipValidationExceptions</name>
    <value>10.1.1.1</value>
  </userDefinedParam>
</userDefinedParameters>
```

For more information about adding IP validation exceptions, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

4. Save the changes.
5. Add execute permissions for the `oamreg.sh` script:

```
chmod u+x /RREG_Home/bin/oamreg.sh
```

Example 15-1 OAM11gRequest.xml for WebCenter Portal Enterprise Deployment

After editing `OAM11gRequest.xml`, the file should contain the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright (c) 2009, 2010, Oracle and/or its affiliates. All rights reserved.
NAME: OAM11GRequest_short.xml - Template for OAM 11G Agent Registration request
file
(Shorter version - Only mandatory values - Default values will be used for all
other fields)
DESCRIPTION: Modify with specific values and pass file as input to the tool.
-->
<OAM11GRegRequest>
  <serverAddress>http://$$oamhost$$:$$oamadminserverport$$</serverAddress>
  <hostIdentifier>$$webtierhost$$_webcenter</hostIdentifier>
  <agentName>$$webtierhost$$_webcenter</agentName>
```

```

<applicationDomain>$$webtierhost$$_webcenter</applicationDomain>
<ipValidation>1</ipValidation>
  <ValList ListName="ipValidationExceptions">
    <ValListMember Value="10.1.1.1"/>
  </ValList>
  <logoutUrls>
    <url>/oamssso/logout.html</url>
  </logoutUrls>
  <protectedResourcesList>
    <resource>/webcenter/adfAuthentication</resource>
    <resource>/integration/worklistapp</resource>
    <resource>/integration/worklistapp/.../*</resource>
  </protectedResourcesList>
  <resource>/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow</resource>
  <resource>/workflow/WebCenterWorklistDetail/faces/adf.task-flow</resource>
  <resource>/workflow/sdpmessagingsca-ui-worklist</resource>
  <resource>/workflow/sdpmessagingsca-ui-worklist/.../*</resource>
  <resource>/sdpmessaging/userprefs-ui</resource>
  <resource>/sdpmessaging/userprefs-ui/.../*</resource>
  <resource>/rss/rssservlet</resource>
  <resource>/owc_discussions/login!withRedirect.jspa</resource>
  <resource>/owc_discussions/login!default.jspa</resource>
  <resource>/owc_discussions/login.jspa</resource>
  <resource>/owc_discussions/admin</resource>
  <resource>/owc_discussions/admin/.../*</resource>
  <resource>/rest/api/resourceIndex</resource>
  <resource>/rest/api/spaces</resource>
  <resource>/rest/api/spaces/.../*</resource>
  <resource>/rest/api/discussions</resource>
  <resource>/rest/api/discussions/.../*</resource>
  <resource>/rest/api/tags</resource>
  <resource>/rest/api/tags/.../*</resource>
  <resource>/rest/api/taggeditems</resource>
  <resource>/rest/api/taggeditems/.../*</resource>
  <resource>/rest/api/activities</resource>
  <resource>/rest/api/activities/.../*</resource>
  <resource>/rest/api/activitygraph</resource>
  <resource>/rest/api/activitygraph/.../*</resource>
  <resource>/rest/api/feedback</resource>
  <resource>/rest/api/feedback/.../*</resource>
  <resource>/rest/api/people</resource>
  <resource>/rest/api/people/.../*</resource>
  <resource>/rest/api/messageBoards</resource>
  <resource>/rest/api/messageBoards/.../*</resource>
  <resource>/rest/api/searchresults</resource>
  <resource>/rest/api/searchresults/.../*</resource>
  <resource>/activitygraph-engines</resource>
  <resource>/activitygraph-engines/.../*</resource>
  <resource>/wcps/api</resource>
  <resource>/wcps/api/.../*</resource>
  <resource>/adfAuthentication</resource>
  <resource>/pagelets/admin</resource>
  <resource>/pagelets/admin/.../*</resource>
  <resource>/pagelets/authenticateWithApplicationServer</resource>
  <resource>/services-producer/adfAuthentication</resource>
  <resource>/em</resource>
  <resource>/em/.../*</resource>
  <resource>/console</resource>
  <resource>/console/.../*</resource>
  <resource>/soa/composer</resource>
  <resource>/soa/composer/.../*</resource>
  <resource>/soa-infra</resource>

```

```

    <resource>/soa-infra/deployer</resource>
    <resource>/soa-infra/deployer/.../*</resource>
    <resource>/soa-infra/events/edn-db-log</resource>
    <resource>/soa-infra/events/edn-db-log/.../*</resource>
    <resource>/soa-infra/cluster/info</resource>
    <resource>/soa-infra/cluster/info/.../*</resource>
    <resource>/inspection.wsil</resource>
    <resource>/cs/idcplg</resource>
    <resource>/cs/idcplg/.../*</resource>
    <resource>/cs/groups</resource>
    <resource>/cs/groups/.../*</resource>
    <resource>/ibr/adfAuthentication</resource>
    <resource>/ibr/adfAuthentication/.../*</resource>
  </protectedResourcesList>
  <publicResourcesList>
    <resource>/webcenter</resource>
    <resource>/webcenter/.../*</resource>
    <resource>/owc_discussions</resource>
    <resource>/owc_discussions/.../*</resource>
    <resource>/rss</resource>
    <resource>/rss/.../*</resource>
    <resource>/workflow</resource>
    <resource>/workflow/.../*</resource>
    <resource>/rest/api/cm/.../*</resource>
    <resource>/pagelets</resource>
    <resource>/services-producer</resource>
    <resource>/wsrp-tools</resource>
    <resource>/cs</resource>
    <resource>/cs/.../*</resource>
    <resource>/ibr</resource>
    <resource>/ibr/.../*</resource>
    <resource>/soa-infra/services/.../*</resource>
    <resource>/soa-infra/directWSDL</resource>
    <resource>/integration/services</resource>
    <resource>/integration/services/.../*</resource>
    <resource>/ucs/messaging/webservice</resource>
    <resource>/ucs/messaging/webservice/.../*</resource>
  </publicResourcesList>
  <excludedResourcesList>
    <resource>/rsscrawl*</resource>
    <resource>/rsscrawl/.../*</resource>
    <resource>/sesUserAuth*</resource>
    <resource>/sesUserAuth/.../*</resource>
    <resource>/services-producer/portlets*</resource>
    <resource>/services-producer/portlets/.../*</resource>
    <resource>/wsrp-tools/portlets*</resource>
    <resource>/wsrp-tools/portlets/.../*</resource>
  </excludedResourcesList>
</OAM11GRegRequest>

```

Note: WebCenter Portal, SOA, and WebCenter Content each provide .conf file that lists their public and protected URI requirements. Instead of specifying public and protect URIs using the `protected_uris=` and `public_uris=` syntax as shown, you can reference each file in turn using the syntax `uris_file=`. For more information and instructions, see "Configuring the WebCenter Portal Policy Domain" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

15.6.4.3 Running the oamreg Tool

1. Run the oamreg tool using the following command:

```
$ ./RREG_Home/bin/oamreg.sh inband input/WebCenterOAM11GRequest.xml
```

2. When prompted for the agent credentials, enter your OAM administrator credentials.

The run should look as follows:

```
-----
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: MW_HOME/Oracle_IDM1/oam/server/rreg/input/WebCenterOAM11gRequest.xml
Enter your agent username:weblogic
Username: weblogic
Enter agent password:
Do you want to enter a Webgate password?(y/n) :
Y
Enter webgate password:
Enter webgate password again:
Password accepted. Proceeding to register..
Aug 16, 2010 1:22:30 AM
oracle.security.am.engines.rreg.client.handlers.request.OAM11GRequestHandler
getWebgatePassword
INFO: Passwords matched and accepted.
Do you want to import an URIs file?(y/n):
n
-----
Request summary:
OAM11G Agent Name:WEBHOST1_webcenter
URL String:WEBHOST1_webcenter
Registering in Mode:inband
Your registration request is being sent to the Admin server at:
http://oamserver.mycompany.com:7001
-----
Inband registration process completed successfully! Output artifacts are created
in the output folder.
```

15.6.4.4 Copying Access files to WEBHOSTS

The following two files are generated in `RREG_Home/output/$$webtierhost$$_webcenter`:

- ObAccessClient.xml
- cwallet.sso

To copy both these files to the WebGate instance location on WEBHOST1 and WEBHOST2:

1. Copy ObAccessClient.xml and cwallet.sso to the WebGate instance directory on WEBHOST1 and WEBHOST2.

For example:

```
scp ObAccessClient.xml oracle@WEBHOSTN:ORACLE_
BASE/admin/webN/config/OHS/ohsN/webgate/config/
```

Where *N* is a sequential number for your installation; for example, 1 for WEBHOST1, 2 for WEBHOST2, and so on.

2. Restart Oracle HTTP Server.

15.6.4.5 Updating REST Policies

REST needs to follow the BASIC authentication scheme so that external clients, such as the Outlook plug-in and iPhone application, can connect to WebCenter REST and be protected with SSO.

To configure the REST end points to use basic authentication:

1. Log in to the Oracle Access Manager console at `http://OAM_HOST:OAM_ADMINSERVER_PORT/oamconsole`.
2. Locate the policy domain that you created and verified in the previous steps and open the **Policies** tab.
3. Go to **Application Domains** > `$$webtierhost$$_webcenter` > **Authentication Policies**.
4. Create a new policy called **WebCenter REST Auth Policy** and choose **Authentication Scheme** as BASIC Scheme.
5. Go to **Application Domains** > `$$webtierhost$$_webcenter` > **Resources**.
6. Search for all the REST resources. Type `/rest*` in the **Resource URL** field and then click **Search**.
7. Edit each REST resource, except for `/rest/api/cmis` entries, and change **Authentication Policy** from **Protected Resource Policy** to **WebCenter REST Auth Policy**.

Figure 15–6 Configuring REST End Points to use Basic Authentication

Resource Type	Host Identif	Resource URL	Query String	Authentication Policy
1 HTTP	we...	/rest/api/cmis*		Public Resource Policy
2 HTTP	we...	/rest/api/cmis/.../*		Public Resource Policy
3 HTTP	we...	/rest/api/discussions/.../*		WebCenter REST Policy
4 HTTP	we...	/rest/api/activities/.../*		WebCenter REST Policy
5 HTTP	we...	/rest/api/messageBoards*		WebCenter REST Policy
6 HTTP	we...	/rest/api/discussions*		WebCenter REST Policy
7 HTTP	we...	/rest/api/spaces*		WebCenter REST Policy
8 HTTP	we...	/rest/api/resourceIndex/.../*		WebCenter REST Policy
9 HTTP	we...	/rest/api/taggeditems*		WebCenter REST Policy
10 HTTP	we...	/rest/api/tags/.../*		WebCenter REST Policy
11 HTTP	we...	/rest/api/taggeditems/.../*		WebCenter REST Policy
12 HTTP	we...	/rest/api/searchresults*		WebCenter REST Policy
13 HTTP	we...	/rest/api/resourceIndex*		WebCenter REST Policy

You should see the following entries:

```

/rest/api/resourceIndex
/rest/api/resourceIndex/.../*
/rest/api/spaces
/rest/api/spaces/.../*
/rest/api/discussions
/rest/api/discussions/.../*
/rest/api/tags
/rest/api/tags/.../*
/rest/api/taggeditems
/rest/api/taggeditems/.../*
/rest/api/activities
/rest/api/activities/.../*
/rest/api/activitygraph
/rest/api/activitygraph/.../*
/rest/api/feedback
/rest/api/feedback/.../*
/rest/api/people
/rest/api/people/.../*
/rest/api/messageBoards
/rest/api/messageBoards/.../*
/rest/api/searchresults
/rest/api/searchresults/.../*

```

15.6.5 Setting Up the WebLogic Authenticators

Set up the WebLogic authenticators by backing up the configuration files, setting up the OAM ID Asserter, and setting the order of providers.

Prerequisite

Before you set up the WebLogic authenticators, you should have already set up the LDAP authenticator by following the steps in [Section 15.2.1, "Creating the LDAP Authenticator."](#) If you have not already created the LDAP authenticator, do it before continuing with this section.

This section includes the following topics:

- [Section 15.6.5.1, "Back Up Configuration Files"](#)
- [Section 15.6.5.2, "Setting Up the OAM ID Asserter"](#)
- [Section 15.6.5.3, "Setting the Order of Providers"](#)

15.6.5.1 Back Up Configuration Files

To be safe, first back up the relevant configuration files stored under WebCenter Portal's Administration Server directory:

```

ORACLE_BASE/admin/domain_name/aserver/domain_name/config/config.xml
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig/jps-con
fig.xml
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig/system-
jazn-data.xml

```

In addition, back up the `boot.properties` file for the Administration Server.

15.6.5.2 Setting Up the OAM ID Asserter

To set up the OAM ID Asserter:

1. Log in as an administrator to Oracle WebLogic Console.

2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, *Default Realm Name*, and then **Providers**.
4. Click **New** and select **OAM Identity Asserter** from the dropdown menu.
5. Name the asserter (for example, **OAM ID Asserter**) and click **Save**.
6. Click the newly added asserter to see the configuration screen for OAM Identity Asserter.
7. Set the control flag to **REQUIRED**.
8. Select both the **ObSSOCookie** and **OAM_REMOTE_USER** options under Chosen types.
9. Save the settings.
10. Finally, connect to the WebLogic domain using WLST and add an OAM SSO provider by running the following command:

```
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",  
logouturi="oamsso/logout.html")
```

15.6.5.3 Setting the Order of Providers

Set the order of providers using the WebLogic Administration Console.

To set the order of the providers:

1. Log in as an administrator to Oracle WebLogic Console.
2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, then the default realm name, and then **Providers**.
4. Reorder the OAM Identity Asserter, OID/OVD Authenticator, and Default Authenticator by ensuring that the control flag for each authenticator is set as follows:
 - OAM Identity Asserter: **REQUIRED**
 - OID LDAP Authenticator (or OVD LDAP Authenticator): **SUFFICIENT**
 - Default Authenticator: **SUFFICIENT**
5. Click **OK**.
6. Click **Activate Changes** to propagate the changes.
7. Restart the Administration Server and all managed servers.

15.6.6 Configuring Virtual Hosts for OAM11g

To configure OAM 11g for virtual hosts we need to bypass single sign-on for applications that only support BASIC authorization or do not require single sign-on.

To configure virtual hosts for OAM 11g:

1. Locate and comment out the following configuration in `webgate.conf`:

```
#<LocationMatch "/*">  
#AuthType Oblix  
#require valid-user  
#</LocationMatch>
```

This entry causes the WebGate to intercept all requests and process them.

2. If the "Default Login page alias" entry appears in `webgate.conf`, comment this out too:

```

#*****Default Login page alias***
#Alias /oamssso "${ORACLE_HOME}/oamssso"
#<LocationMatch "/oamssso/*">
#Satisfy any
#</LocationMatch>
#*****

```

3. Edit the virtual host configuration section as follows:

```

NameVirtualHost *:7777

<VirtualHost *:7777>
ServerName https://wcp.mycompany.com:443
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
</VirtualHost>

<VirtualHost *:7777>
ServerName admin.mycompany.com:80
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
</VirtualHost>

<VirtualHost *:7777>
ServerName wcpinternal.mycompany.com:80
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
</VirtualHost>

#Virtual host for SharePoint access
<VirtualHost *:7777>
ServerName wcp-spaces.mycompany.com
ServerAdmin you@your.address
RewriteEngine On
RewriteOptions inherit

#SharePoint entry point
<Location />
WebLogicCluster WCPHOST1:9000,WCPHOST2:9000
SetHandler weblogic-handler
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

# Spaces Application
<Location /webcenter>
Deny from all
</Location>

<Location /webcenterhelp>
Deny from all

```

```

</Location>

  <Location /rss>
    Deny from all
  </Location>

  <Location /rest>
    Deny from all
  </Location>

</VirtualHost>

```

4. Restart Oracle HTTP Server.

15.7 Configuring WebCenter Portal Applications for SSO

This section covers the following topics:

- [Section 15.7.1, "Configuring System Properties for WebCenter Portal: Spaces"](#)
- [Section 15.7.2, "Configuring the WebCenter Portal: Spaces Administrator Role"](#)
- [Section 15.7.3, "Setting Up Discussions Server to Use OAM as SSO Provider"](#)

15.7.1 Configuring System Properties for WebCenter Portal: Spaces

Configure the Spaces application for SSO by adding a setting to `EXTRA_JAVA_PROPERTIES`.

The `oracle.webcenter.spaces.osso` system property tells WebCenter Portal and ADF that the application is configured in SSO mode and some special handling is required. The following system property is required:

Table 15–4 System Property

Property	Value	Comment
<code>oracle.webcenter.spaces.osso</code>	<code>true</code>	This flag tells WebCenter Portal that SSO is being used, so no login form should be displayed on the default landing page. Instead, it displays a login link that the user can click to invoke the SSO authentication.

To set this property for the Spaces application on `WCPHOST1` and `WCPHOST2`, edit the `setDomainEnv.sh` script located in your `managedserver_domain_home/bin` directory. Add the property to the `EXTRA_JAVA_PROPERTIES` variable, as follows:

```

EXTRA_JAVA_PROPERTIES="-Doracle.webcenter.spaces.osso=true ${EXTRA_JAVA_
PROPERTIES}"
export EXTRA_JAVA_PROPERTIES

```

15.7.2 Configuring the WebCenter Portal: Spaces Administrator Role

After Oracle Internet Directory or Oracle Virtual Directory is configured as the primary authenticator in the Spaces application, the default user "weblogic" should not be used as the Spaces administrator. Create a user in Oracle Internet Directory and make that user the Spaces administrator, either using WLST or Enterprise Manager:

- [Section 15.7.2.1, "Granting the Spaces Administrator Role Using WLST"](#)

- [Section 15.7.2.2, "Granting the Spaces Administrator Role Using Fusion Middleware Control"](#)

15.7.2.1 Granting the Spaces Administrator Role Using WLST

To grant the Spaces Administrator role using WLST:

1. Navigate to your WebCenter Portal Oracle home directory and invoke the WLST script:

```
(UNIX) MW_HOME/wc/common/bin/wlst.sh
```

```
(Windows) MW_HOME\wc\common\bin\wlst.cmd
```

2. Connect to the Administration Server for the target domain with the following command:

```
wls:/offline>connect("user_name","password","host_name:port_number")
```

Where:

- *user_name* is the name of the user account with which to access the Administration Server (for example, *weblogic*)
 - *password* is the password with which to access the Administration Server
 - *host_id* is the host ID of the Administration Server
 - *port* is the port number of the Administration Server (for example, 7001).
3. Create a user in the LDAP Store named **WCAdmin**.
This user will be assigned the Spaces Administrator role.
 4. Grant the Spaces administrator application role to the user in LDAP using the `grantAppRole` command.

For example:

```
grantAppRole(appStripe="webcenter", appRoleName="s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator",
principalClass="weblogic.security.principal.WLSUserImpl",
principalName="WCAdmin")
```

where **WCAdmin** is the name of the administrator account.

Note: Before `grantAppRole` is called, **WCAdmin** must exist in LDAP. For user creation details, see [Section 15.2.2.1, "Provisioning Admin Users and Groups in an LDAP Directory."](#)

5. To test the new account, log in to the Spaces application using the new account name.

The Administration link should appear, and you should be able to perform all administrator operations.

15.7.2.2 Granting the Spaces Administrator Role Using Fusion Middleware Control

This section describes how to grant the Spaces administrator role to a user account other than the default *weblogic* account.

To grant the Spaces Administrator role using Fusion Middleware Control:

1. Log into Fusion Middleware Control and navigate to the home page for Spaces.

2. From the **WebCenter Portal** menu, select **Security**, and then **Application Roles**.
The Application Roles page displays.
3. Search for the Spaces Administrator role:
 - a. Select the **Select Application Stripe to Search** check box.
 - b. Choose **webcenter** (the name of the Spaces application).
 - c. In the **Role Name** field, enter `s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator`, and then click the **Search** (arrow) icon.
4. Click the administrator role name (`s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator`) in the Role Name column.
The Edit Application Role page displays.
5. Click **Add User**.
The Add User pop-up displays.
6. Use the Search function to search for the user to assign the Administrator role to.
7. Use the arrow keys to move the user from the Available Users column to the Selected Users column, and click **OK**.
8. On the Edit Application Role page, click **OK**.
9. Restart the `WC_Spaces` managed server.
When you log in to the Spaces application, the Administration link should appear and you should be able to perform all administrator operations.

15.7.3 Setting Up Discussions Server to Use OAM as SSO Provider

This section contains the following topics:

- [Section 15.7.3.1, "Granting Administrator Permissions on the Discussions Server"](#)
- [Section 15.7.3.2, "Configuring System Properties for Discussions Server"](#)

15.7.3.1 Granting Administrator Permissions on the Discussions Server

When associating the domain with an identity store that does not contain the group "Administrators", you must assign some other valid user or group the administrator role for the discussions server.

The WLST command `addDiscussionsServerAdmin` lets you grant system administrator permissions on the Discussions server to a user or a group. For command syntax and examples, see the section, "addDiscussionsServerAdmin" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For example,

1. Connect to the Administration Server:

For example:

```
cd $MW_HOME/wc/common/bin/
./wlst.sh

connect("weblogic", "weblogic", "ADMINHOST:7001")
```

2. Grant administration permissions to a user or a group:

```
addDiscussionsServerAdmin(appName='owc_discussions', name='weblogic_wc',
```



```
type='USER', server='wc_collaboration1')
```

or:

```
addDiscussionsServerAdmin(appName='owc_discussions',
name='discussions-admin-group', type='GROUP', server='wc_collaboration1')
```

Where *weblogic_wc* and *discussions-admin-group* are example user/groups that you want to assign the administrator role for the discussions server.

For command syntax and examples, see the section, "addDiscussionsServerAdmin" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

15.7.3.2 Configuring System Properties for Discussions Server

To configure Oracle WebCenter Discussions Server for OAM single sign-on:

1. Log in to the Oracle WebCenter Discussions Server Admin Console at:
`http://wcpinternal.mycompany.com/owc_discussions/admin`
2. Open the System Properties page and edit, (if it already exists), or add the `owc_discussions.sso.mode` property, setting its value to `true`.
3. Edit or add the `jiveURL` property to point to the base URL of the web tier for the SSO server. For example:

```
jiveURL = idmhost.example.com:8890/owc_discussions
```

15.8 Configuring WebCenter Portal and BPEL Authentication

This section covers the following topics:

- [Section 15.8.1, "Verify Authenticators"](#)
- [Section 15.8.2, "Set Role Members for BPMWorkflowAdmin Application Role in soa-infra"](#)
- [Section 15.8.3, "Configure SOA Callback URLs"](#)

15.8.1 Verify Authenticators

Ensure that the SOA domain is using the same authenticators as the WebCenter Portal domain and has been configured for OAM Authentication.

15.8.2 Set Role Members for BPMWorkflowAdmin Application Role in soa-infra

When associating the domain with a identity store that does not contain the default user `weblogic`, you must assign some other valid user to the application role `BPMWorkflowAdmin`.

To grant `BPMWorkflowAdmin` to a valid user:

1. Create a user in LDAP Store, in this example `WCAdmin`, who will be assigned the role.
2. Assign the `BPMWorkflowAdmin` role using WLST. This can be done using `wlst` from the SOA Oracle home:

For example:

```
cd ORACLE_HOME/common/bin/
wlst.sh
```

```
connect("weblogic","weblogic", "ADMINHOST:7001")
revokeAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="SOAdmin")
grantAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
principalClass="weblogic.security.principal.WLSUserImpl",
principalName="WCAdmin")
```

15.8.3 Configure SOA Callback URLs

For the Worklist service to work properly when Oracle Access Manager is enabled, it is mandatory that SOA callback URLs are configured correctly. For information about callback URLs, see [Section 9.7.3, "Setting the Frontend HTTP Host and Port."](#)

For SOA applications, the following callback URLs must be set to `http://wcpinternal.mycompany.com`:

- **Callback Server URL**
- **Server URL**

To modify these URLs using Fusion Middleware Control:

1. Select **Farm_wcpedg_domain, SOA, soa-infra (wls_soa1), SOA, Infrastructure, SOA Administration**, and then **Common Properties**.
2. Enter **http://wcpinternal.mycompany.com**.
3. Restart the SOA servers.

15.9 Backing Up the Identity Management Configuration

After you have verified that the extended domain is working, back up the domain configuration. This is a quick backup for the express purpose of immediate restore in case of failures in future procedures. Back up the configuration to the local disk. This backup can be discarded once you have completed the enterprise deployment. Once you have completed the enterprise deployment, you can initiate the regular deployment-specific backup and recovery process.

For information about backing up the environment, see "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*. For information about recovering your information, see "Recovering Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

To back up the configuration at this point:

1. Back up the web tier:
 - a. Shut down the instance using `opmnctl`.

```
ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
```
 - 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 using `opmnctl`:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl startall
```

2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or OS tools such as `tar` for cold backups if possible.
3. Back up the Administration Server domain directory to save your domain configuration. The configuration files are located in the following directory:

```
ORACLE_BASE/ admin/domain_name
```

To back up the Administration Server run the following command on SOHOST1:

```
tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the topology. These operations include monitoring, scaling, and backing up your topology.

This chapter contains the following sections:

- [Section 16.1, "Overview of Managing Monitoring the Topology"](#)
- [Section 16.2, "Managing Space in the SOA Infrastructure Database"](#)
- [Section 16.3, "Configuring UMS Drivers"](#)
- [Section 16.4, "Scaling Up the Topology \(Adding Managed Servers to Existing Nodes\)"](#)
- [Section 16.5, "Scaling Out the Topology \(Adding Managed Servers to New Nodes\)"](#)
- [Section 16.6, "Performing Backups and Recoveries in WebCenter Portal Deployments"](#)
- [Section 16.7, "Preventing Timeouts for SQLNet Connections"](#)
- [Section 16.8, "Troubleshooting Oracle WebCenter Portal Enterprise Deployments"](#)

16.1 Overview of Managing Monitoring the Topology

After configuring the WebCenter Portal enterprise deployment, use the information in this chapter to manage the topology.

For information on monitoring the topology and WebCenter Portal applications, see "Monitoring Oracle WebCenter Portal Performance" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

At some point you may need to expand the topology by scaling it up, or out. See [Section 16.4, "Scaling Up the Topology \(Adding Managed Servers to Existing Nodes\)"](#) and [Section 16.5, "Scaling Out the Topology \(Adding Managed Servers to New Nodes\)"](#) for information about the difference between scaling up and scaling out, and instructions for performing these tasks.

Back up the topology before and after any configuration changes. [Section 16.6, "Performing Backups and Recoveries in WebCenter Portal Deployments"](#) provides information about the directories and files that should be back up to protect against failure as a result of configuration changes.

This chapter also documents solutions for possible known issues that may occur after you have configured the topology.

16.2 Managing Space in the SOA Infrastructure Database

Although not all composites may use the database frequently, the service engines generate a considerable amount of data in the CUBE_INSTANCE and MEDIATOR_INSTANCE schemas. Lack of space in the database may prevent SOA composites from functioning.

To manage space in the SOA infrastructure database:

- Watch for generic errors, such as "oracle.fabric.common.FabricInvocationException" in the Oracle Enterprise Manager Fusion Middleware Control console (dashboard for instances).
- Search in the SOA server's logs for errors, such as:

```
Error Code: 1691
...
ORA-01691: unable to extend lob segment
SOAINFRA.SYS_LOB0000108469C00017$$ by 128 in tablespace SOAINFRA
```

These messages are typically indicators of space issues in the database that may likely require adding more data files or more space to the existing files. The SOA Database Administrator should determine the extension policy and parameters to be used when adding space.

- Purge old composite instances to reduce the SOA Infrastructure database's size. Oracle does not recommend using the Oracle Enterprise Manager Fusion Middleware Control for this type of operation. In most cases the operations cause a transaction time out. There are specific packages provided with the Repository Creation Utility to purge instances. For example:

```
DECLARE
  FILTER INSTANCE_FILTER := INSTANCE_FILTER();

  MAX_INSTANCES NUMBER;
  DELETED_INSTANCES NUMBER;
  PURGE_PARTITIONED_DATA BOOLEAN := TRUE;
BEGIN
  .
  FILTER.COMPOSITE_PARTITION_NAME:="default";
  FILTER.COMPOSITE_NAME := "FlatStructure";
  FILTER.COMPOSITE_REVISION := "10.0";
  FILTER.STATE := fabric.STATE_UNKNOWN;
  FILTER.MIN_CREATED_DATE := to_timestamp("2010-09-07", "YYYY-MM-DD");
  FILTER.MAX_CREATED_DATE := to_timestamp("2010-09-08", "YYYY-MM-DD");
  MAX_INSTANCES := 1000;
  .
  DELETED_INSTANCES := FABRIC.DELETE_COMPOSITE_INSTANCES(
    FILTER => FILTER,
    MAX_INSTANCES => MAX_INSTANCES,
    PURGE_PARTITIONED_DATA => PURGE_PARTITIONED_DATA
  );
;
```

This deletes the first 1000 instances of the FlatStructure composite (version 10) created between '2010-09-07' and '2010-09-08' that are in "UNKNOWN" state. For more information on the possible operations included in the SQL packages provided, see "Managing SOA Composite Applications" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*. Always use the scripts provided for a correct purge. Deleting rows in just the **composite_dn** table may leave dangling references in other tables used by the Oracle Fusion Middleware SOA Infrastructure.

16.3 Configuring UMS Drivers

UMS driver configuration is not automatically propagated in a SOA cluster. To propagate UMS driver configuration in a cluster:

- Apply the UMS driver configuration in each server in the Enterprise Deployment topology that is using the driver.
- If you are using server migration, servers are moved to a different node's domain directory. Pre-create the UMS driver configuration in the failover node. The UMS driver configuration file is located in the following directory:

```
ORACLE_BASE/admin/domain_name/msserver/domain_name/servers/server_name/ tmp/_WL_
user/ums_driver_name/*/configuration/driverconfig.xml
```

Where '*' represents a directory name that is randomly generated by Oracle WebLogic Server during deployment. For example, 3682Yq.

Create the UMS driver configuration file in preparation for possible failovers by forcing a server migration, and copy the file from the source node.

It is required to restart the driver for these changes to take effect (that is, for the driver to consume the modified configuration). To restart the driver:

1. Log on to the Oracle WebLogic Administration Console.
2. Expand the environment node on the navigation tree.
3. Click on **Deployments**.
4. Select the driver.
5. Click **Stop->When work completes** and confirm the operation.
6. Wait for the driver to transition to the "Prepared" state (refresh the administration console page, if required).
7. Select the driver again, and click **Start->Servicing all requests** and confirm the operation.

Verify in Oracle Enterprise Manager Fusion Middleware Control that the properties for the driver have been preserved.

16.4 Scaling Up the Topology (Adding Managed Servers to Existing Nodes)

When you scale up the topology, you add new managed servers to nodes that are already running one or more managed servers. You can use the existing node installations (such as WebLogic Server home, Oracle Fusion Middleware home, and domain directories), when you create the new managed servers. You do not need to install WebLogic Server, SOA or WebCenter Portal binaries at a new location or to run pack and unpack.

When you scale up a server that uses server migration, plan for your appropriate capacity and resource allocation needs. Take the following scenario for example:

- Server1 exists in node1 and uses server migration in its cluster with server2 on node2.
- Server3 is added to the cluster in node1 in a scale up operation. It also uses server migration.

In this scenario, a situation may occur where all servers (server1, server2, server3 and admin server) end up running in a node1 or node2. This means each node needs to be designed with enough resources to sustain the worst case scenario where all servers using server migration end in one single node (as defined in the server migration candidate machine configuration).

16.4.1 Scaling up Oracle SOA (includes WSM)

To scale up the SOA topology (includes WSM):

1. Using the Oracle WebLogic Server Administration Console, clone WLS_SOA1 or WLS_WSM1 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. 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.
- b. Click **Lock & Edit** and select the managed server that you want to clone (for example, WLS_SOA1).
- c. Click **Clone**.
- d. Name the new managed server WLS_SOAn, where *n* is a number that identifies the new managed server. In this case, you are adding a new server to Node 1, where WLS_SOA1 was running.

For the remainder of the steps, you are adding a new server to SOAHOST1, which is already running WLS_SOA1.

2. For the listen address, assign the host name or IP to use for this new managed server. If you are planning to use server migration as recommended for this server, enter 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. For WLS_WSM servers, run the Java Object Cache configuration utility again to include the new server in the JOC distributed cache as described in [Section 8.5.5, "Configuring the Java Object Cache for Oracle WSM."](#) You can use the same discover port for multiple WLS_WSM servers in the same node. Repeat the steps provided in [Section 8.5.5, "Configuring the Java Object Cache for Oracle WSM"](#) for each WLS_WSM server and the server list is updated.
4. Create JMS servers for SOA 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 (which will be created in a later step) and name it, for example, **SOAJMSFileStore_N**. Specify the path for the store as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#) as the directory for the JMS persistent stores:

```
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 will fail.

- b. Create a new JMS server for SOA: for example, **SOAJMS**Server_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 UMS JMS server (which will be created in a later step) and name it, for example, **UMSJMS**FileStore_N. Specify the path for the store as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#) as the directory for the JMS persistent stores:

```
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 will fail.

Note: 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, **UMSJMS**Server_N. Use the UMSJMSFileStore_N for this JMS server. Target the UMSJMSServer_N server to the recently created managed server (WLS_SOAn).
- e. **For BPM Systems only:** Create a new persistence store for the new BPMJMSServer, for example, **BPMJMS**FileStore_N. Specify the path for the store. This should be a directory on shared storage as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#):

```
ORACLE_BASE/admin/domain_name/cluster_name/jms/BPMJMSFileStore_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 BPM JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- f. **For BPM systems only:** Create a new JMS Server for BPM, for example, BPMJMSServer_N. Use the BPMJMSFileStore_N for this JMSServer. Target the BPMJMSServer_N Server to the recently created Managed Server (WLS_SOAn).
- g. Target the UMSJMSSystemResource to the SOA_Cluster as it may have changed during extend operations. 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 UMSJMSSytemResource and open the Targets tab. Make sure all of the servers in the SOA_Cluster appear selected (including the recently cloned WLS_SOAn).
- h. Update the SubDeployment Targets for SOA, UMS and BPM JMS Modules (if applicable) to include the recently created JMS servers.

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 on the JMS module (for SOA: SOAJMSModule, for BPM: BPMJMSModule and for UMS: UMSSystemResource) represented as a hyperlink in the **Names** column of the table. The Settings page for module appears. Open the **SubDeployments** tab. The subdeployment for the deployment module appears.

Note: This subdeployment module name is a random name in the form of SOAJMSServerXXXXXX, UMSJMSServerXXXXXX, or BPMJMSServerXXXXXX, resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click on it. Add the new JMS Server (for UMS add UMSJMSServer_N, for SOA add SOAJMSServer_N). Click **Save and Activate**.

5. Configuring Oracle Coherence for deploying composites for the new server as described in [Section 9.4, "Configuring Oracle Coherence for Deploying Composites."](#)

Note: Only the **localhost** field must be changed for the server. Replace the localhost with the listen address of the new server added:

```
Dtangosol.coherence.localhost=SOAHOST1VHNn
```

6. Configure the persistent store for the new server. This should be a location visible from other nodes as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#).

From the Administration Console, select the **Server_name**, and then the **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.

7. 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 SOAHOST*n*.

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 Fusion Middleware 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 server appears.

- e. Click the **SSL** tab.

- f. Click **Advanced**.
 - g. Set Hostname Verification to **None**.
 - h. Click **Save**.
8. Configure server migration for the new managed server. To configure server migration using the Oracle WebLogic Server Administration Console:

Note: Because this is a scale-up operation, the node should already contain a Node Manager and environment configured for server migration that includes netmask, interface, wlsifconfig script superuser privileges, and so on. The floating IP for the new SOA managed server should also be already present.

- a. In the Domain Structure window, expand the **Environment** node and then click **Servers**. The Summary of Servers page appears.
- b. Click the name of the server (represented as a hyperlink) in Name column of the table for which you want to configure migration. The settings page for the selected server appears.
- c. Click the **Migration** subtab.
- d. In the Migration Configuration section, select the servers that participate in migration in the Available window by clicking the right arrow. Select the same migration targets as for the servers that already exist on the node.

For example, for new managed servers on SOAHOST1, which is already running WLS_SOA1, select SOAHOST2. For new managed servers on SOAHOST2, which is already running WLS_SOA2, select SOAHOST1.

Note: The appropriate resources must be available to run the managed servers concurrently during migration.

- e. Choose the **Automatic Server Migration Enabled** option. This enables the Node Manager to start a failed server on the target node automatically.
 - f. Click **Save**.
 - g. Restart the Administration Server, managed servers, and Node Manager.
To restart the Administration Server, use the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)
9. Update the cluster address to include the new server:
- a. In the Administration Console, select **Environment**, and then **Cluster**.
 - b. Click the **SOA_Cluster** server.
The Settings screen for the SOA_Cluster appears.
 - c. Click **Lock & Edit**.
 - d. Add the new server's address and port to the **Cluster address** field. For example:
ADMINVHN:8011,SOAHOST2VHN1:8011,SOAHOST1VHN1:8001
 - e. Save and activate the changes.

10. Test server migration for this new server. To test migration, perform the following 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 PID of the managed server. You can identify the PID of the node using `ps -ef | grep WLS_SOAn`.
 - b. Monitor the Node Manager Console for a message indicating that WLS_SOAn's floating IP has been disabled.
 - c. Wait for the Node Manager to attempt 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. Node Manager logs a message indicating that the server will not be restarted again locally.

16.4.2 Scaling Up WebCenter Portal

To scale up the WebCenter Portal topology:

Note: Running multiple managed servers on one node is only supported for **WC_Spaces** and **WC_Portlet** servers.

1. Using the WebLogic Server Administration Console, clone WC_Spaces1 or WC_Portlet1 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. In the Administration Console, select **Environment**, and then **Servers**.
- b. Click **Lock & Edit**.
- c. Select the managed server that you want to clone, for example, **WC_Spaces1** or **WC_Portlet1**.
- d. Select **Clone**.
- e. Name the new managed server `WC_SERVERNAME n` , where n is a number to identify the new managed server.

For the remainder of the steps, you add the new server to WCPHOST1, which is already running WC_Spaces1 or WC_Portlet1.

2. For the listen address, assign the host name or IP to use for this new managed server, which should be the same as an existing server.

Ensure that the port number for this managed server is available on this node.
3. Add the new managed server to the Java Object Cache Cluster. For details, see [Section 10.5, "Configuring the Java Object Cache for Spaces_Cluster."](#)
4. Reconfigure the Oracle HTTP Server module with the new member in the cluster. For more information see [Section 10.11.1, "Configuring Oracle HTTP Server for the WC_Spaces \$n\$, WC_Portlet \$n\$, WC_Uilities \$n\$, and WC_Collaboration \$n\$ Managed Servers."](#) Add the host and port of the new server to the end of the `WebLogicCluster` parameter.
 - For WC_Spaces, add the member to the Location blocks for `/webcenter`, `/webcenterhelp`, `/rss`, `/rest`, `/wcsdocs`.

- For WC_Portlet, add the member to the Location blocks for /portalTools, /wsrp-tools, /richtextportlet, /pageletadmin, /wcps.

16.5 Scaling Out the Topology (Adding Managed Servers to New Nodes)

When you scale out the topology, you add new managed servers configured with SOA and or WSM-PM to new nodes.

Before performing the steps in this section, check that you meet these requirements:

Prerequisites

- There must be existing nodes running managed servers configured with SOA and WSM-PM 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.)
- When an ORACLE_HOME or WL_HOME is shared by multiple servers in different nodes, keep 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 the attachHome.sh script in the following location:

```
ORACLE_HOME/oui/bin/
```

To update the Middleware home list to add or remove a WL_HOME, edit the beahomelist file located in the following directory:

```
user_home/boa/
```

16.5.1 Scaling out Oracle SOA (includes WSM)

To scale out the topology:

1. On the new node, mount the existing MW_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 from SOAHOST*n*:

```
cd ORACLE_COMMON_HOME/oui/bin/attachHome.sh
./attachHome.sh -jreLoc ORACLE_BASE/fmw/jrockit_160_<version>
```

To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the \$HOME/boa/beahomelist file and add MW_HOME to it.

3. Log in to the Oracle WebLogic Administration Console.
4. Create a new machine for the new node that will be used, and add the machine to the domain.
5. Update the machine's Node Manager's address to map the IP of the node that is being used for scale out.

6. Use the Oracle WebLogic Server Administration Console to clone WLS_SOA1/WLS_WSM1 into a new managed server. Name it WLS_SOAn/WLS_WLS_WSMn, 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.

7. Assign the host name or IP to use for the new managed server for the listen address of the managed server.

If you are planning to use server migration for this server (which Oracle recommends) this should be the VIP (also called a floating IP) for the server. This VIP should be different from the one used for the existing managed server.

8. For WLS_WSM servers, run the Java Object Cache configuration utility again to include the new server in the JOC distributed cache as described in [Section 8.5.5, "Configuring the Java Object Cache for Oracle WSM."](#)
9. Create JMS Servers for SOA, BPM, (if applicable) and UMS on the new managed server.

Note: These steps are not required for scaling out the WLS_WSM managed server, only for WLS_SOA managed servers.

Create the JMS servers for SOA and UMS as follows:

- a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMServer (which will be created in a later step) and name it, for example, **SOAJMSFileStore_N**. Specify the path for the store as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#) as the directory for the JMS persistent stores:

```
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 will fail.

- b. Create a new JMS server for SOA, for example, SOAJMServer_N. Use the SOAJMSFileStore_N for this JMS server. Target the SOAJMServer_N Server to the recently created managed server (WLS_SOAn).
- c. Create a new persistence store for the new UMSJMServer, and name it, for example, **UMSJMSFileStore_N**. As the directory for the persistent store, specify the path recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#) as the directory for the JMS persistent stores:

```
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 will fail.

Note: 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. **For BPM Systems only:** Create a new persistence store for the new BPMJMSServer, for example, **BPMJMSFileStore_N**. Specify the path for the store. This should be a directory on shared storage as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#).

ORACLE_BASE/admin/domain_name/cluster_name/jms/BPMJMSFileStore_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 BPM JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- f. **For BPM systems only:** Create a new JMS Server for BPM, for example, BPMJMSServer_N. Use the BPMJMSFileStore_N for this JMSServer. Target the BPMJMSServer_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 SOAJMSModuleUDDs (represented as a hyperlink in the Names column of the table). The Settings page for SOAJMSModuleUDDs appears. Open the SubDeployments tab. The SOAJMSSubDM subdeployment appears.

Note: This subdeployment module results from updating the JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2) with the Uniform Distributed Destination Script (*soa-createUDD.py*), which is required for the initial Enterprise Deployment topology setup.

Click on it. Add the new JMS server for SOA called SOAJMSServer_N to this subdeployment. Click **Save**.

- h. Target the UMSJMSSystemResource to the SOA_Cluster as it may have changed during extend operations. 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 UMSJMSSytemResource and open the Targets tab. Make sure all of the servers in the SOA_Cluster appear selected (including the recently cloned WLS_SOAn).

- i. Update the SubDeployment Targets for SOA, UMS and BPM JMS Modules (if applicable) to include the recently created JMS servers.

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 on the JMS module (for SOA: SOAJMSModule, for BPM: BPMJMSModule and for UMS: UMSSystemResource) represented as a hyperlink in the **Names** column of the table. The Settings page for module appears. Open the **SubDeployments** tab. The subdeployment for the deployment module appears.

Note: This subdeployment module name is a random name in the form of SOAJMSModuleXXXXXX, UMSSystemResourceXXXXXX, or BPMJMSModuleXXXXXX, resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click on it. Add the new JMS Server (for UMS add UMSSystemResource_N, for SOA add SOAJMSModule_N). Click **Save and Activate**.

10. Run the `pack` command on SOAHOST1 to create a template pack as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name
-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_COMMON_HOME/common/bin
```

Run the `unpack` command on SOAHOST*n* to unpack the template in the managed server domain directory as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=ORACLE_BASE/admin/domain_name
/mserver/domain_name/
-template=soadomaintemplateScale.jar
-app_dir=ORACLE_BASE/admin/domain_name/mserver/apps
```

11. Configuring Oracle Coherence for deploying composites for the new server as described in [Section 9.4, "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:

```
Dtangosol.coherence.localhost=SOAHOST1VHNn
```

12. Configure the persistent store for the new server. This should be a location visible from other nodes as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment"](#).

From the Administration Console, select the **Server_name**, and then the **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.

13. Disable host name verification for the new managed server. Before starting and verifying the WLS_SOA n managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in SOAHOST n .

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 Fusion Middleware Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
 - b. Expand the **Environment** node in the **Domain Structure** window.
 - c. Click **Servers**.
The Summary of Servers page appears.
 - d. Select WLS_SOA n in the **Names** column of the table.
The Settings page for server appears.
 - e. Click the **SSL** tab.
 - f. Click **Advanced**.
 - g. Set Hostname Verification to **None**.
 - h. Click **Save**.
14. Start Node Manager on the new node. To start 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
```

15. Start and test the new managed server from the Oracle WebLogic Server Administration Console.
 - a. Ensure that the newly created managed server, WLS_SOA n , is running.
 - b. Access the application on the load balancer (<https://soa.mycompany.com/soa-infra>). The application should be functional.

Note: The HTTP Servers in the topology should round robin requests to the newly added server (a few requests, depending on the number of servers in the cluster, may be required to hit the new server). It is not required to add all servers in a cluster to the WebLogicCluster directive in Oracle HTTP Server's `mod_wl_ohs.conf` file. However, routing to new servers in the cluster takes place only if at least one of the servers listed in the WebLogicCluster directive is running.

16. Configure server migration for the new managed server.

Note: Because this new node uses an existing shared storage installation, the node already is using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP for the new SOA Managed Server is already present in the new node.

Log into the Oracle WebLogic Server Administration Console and configure server migration:

- a. Expand the **Environment** node in the Domain Structure windows and then choose Servers. The Summary of Servers page appears.
- b. 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.
- c. Click the **Migration** tab.
- d. In the Available field of the Migration Configuration section, click the right arrow to select the machines to which to allow migration.

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.

- e. Select **Automatic Server Migration Enabled**. This enables the Node Manager to start a failed server on the target node automatically.
 - f. Click **Save**.
 - g. Restart the Administration Server, managed servers, and the Node Manager. To restart the Administration Server, use the procedure in [Section 8.4.3, "Starting the Administration Server on SOAHOST1."](#)
17. Update the cluster address to include the new server:
- a. In the Administration Console, select **Environment**, and then **Cluster**.
 - b. Click the **SOA_Cluster** server.
The Settings screen for the SOA_Cluster appears.
 - c. Click **Lock & Edit**.

- d. Add the new server's address and port to the **Cluster address** field. For example:
ADMINVHN:8011,SOAHOST2VHN1:8011,SOAHOSTNVHN1:8001
 - e. Save and activate the changes.
18. Test server migration for this new server from the node where you added the new server:
- a. Stop the **WLS_SOAn** managed server by running the following command on the PID (process ID) of the managed server:

```
kill -9 pid
```

You can identify the PID of the node using the following command:

```
ps -ef | grep WLS_SOAn
```

Note: For Windows, you can terminate the Managed Server using the `taskkill` command. For example:

```
taskkill /f /pid pid
```

Where *pid* is the process ID of the Managed Server.

To determine the process ID of the WLS_SOAn Managed Server, run the following command:

```
MW_HOME\jrockit_160_20_D1.0.1-2124\bin\jps -l -v
```

- b. In the Node Manager Console you should see a message indicating that WLS_SOAn's floating IP 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.

16.5.2 Scaling Out Oracle WebCenter Portal

In scaling out your topology, you add new managed servers, configured with Oracle WebCenter Portal applications, to new nodes.

Before performing the steps in this section, check that you meet these requirements:

Prerequisites

- There must be existing nodes running managed servers configured with WebCenter Portal within the topology.
- The new node can access the existing home directories for WebLogic Server and Oracle WebCenter Portal. You use the existing installations in shared storage for creating a new managed server. There is no need to install WebLogic Server or WebCenter Portal binaries in a new location, although you need to run `pack` and `unpack` to create a managed server domain.

- Both WC_Spaces and WC_Uutilities servers must be scaled out or not scaled out on the new node. This is because of the local affinity between WebCenter Portal: Spaces and the Analytics application.

To scale out the topology:

- On the new node, mount the existing Middleware home, which should include the WebCenter Portal installation and the domain directory, and ensure that the new node has access to this directory, just as the rest of the nodes in the domain do.
- Attach ORACLE_HOME in shared storage to the local Oracle Inventory, execute the following commands:

```
WCPHOSTn> cd ORACLE_BASE/product/fmw/wc/
WCPHOSTn> ./attachHome.sh -jreLoc ORACLE_BASE/fmw/jrockit_160_<version>
```

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.

- Log in to the Oracle WebLogic Administration Console.
- Create a new machine for the new node that will be used, and add the machine to the domain.
- Update the machine's Node Manager's address to map the IP address of the node that is being used for scale out.
- Use the Oracle WebLogic Server Administration Console to clone either WC_Spaces1 or WC_Portlet1 or WC_Collaboration1 or WC_Uutilities1 into a new managed server. Name it WC_XXXn, where n is a number and assign it to the new machine.
- For the listen address, assign the host name or IP to use for the new managed server. Perform these steps to set the managed server listen address:
 - Log into the Oracle WebLogic Server Administration Console.
 - In the **Change Center**, click **Lock & Edit**.
 - Expand the **Environment** node in the **Domain Structure** window.
 - Click **Servers**. The Summary of Servers page appears.
 - Select the managed server with the listen address you want to update in the **Names** column of the table. The Setting page for that managed server appears.
 - Set the **Listen Address** to WCPHOSTn where WCPHOSTn is the DNS name of your new machine.
 - Click **Save**.
 - Save and activate the changes.

The changes do not take effect until the managed server is restarted.

- Run the pack command on SOAHOST1 to create a template pack and unpack onto WCPHOSTn.

These steps are documented in [Section 10.4.1, "Propagating the Domain Configuration to SOAHOST2, WCPHOST1, and WCPHOST2 Using the unpack Utility."](#)

- 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:

```
WCPHOSTn> WL_HOME/server/bin/startNodeManager new_node_ip
```

10. If this is a new Collaboration managed server:
 - a. Ensure that you have followed the steps in [Section 10.7, "Configuring Clustering on the Discussions Server,"](#) to configure clustering for the new Discussions Server.
 - b. Ensure also that the steps in [Section 10.6, "Converting Discussions from Multicast to Unicast"](#) are performed, using the hostname of the new host for the `coherence.localhost` parameter.
11. If this is a new Utilities managed server, ensure that Activity Graph is disabled by following the steps in [Section 10.9, "Configuring Activity Graph."](#) Ensure also that the steps for configuring a new Analytics Collector in [Section 10.8, "Configuring Analytics"](#) have been followed for the Utilities and the local Spaces Server.
12. Start and test the new managed server from the Oracle WebLogic Server Administration Console:
 - a. Ensure that the newly created managed server, `WLS_SOAn`, is running.
 - b. Access the application on the load balancer (<https://soa.mycompany.com/soa-infra>). The application should be functional.

Note: The HTTP Servers in the topology should round robin requests to the newly added server (a few requests, depending on the number of servers in the cluster, may be required to hit the new server). It is not required to add all servers in a cluster to the `WebLogicCluster` directive in Oracle HTTP Server's `mod_wl_ohs.conf` file. However, routing to new servers in the cluster takes place only if at least one of the servers listed in the `WebLogicCluster` directive is running.

16.6 Performing Backups and Recoveries in WebCenter Portal Deployments

[Table 16–1](#) lists the static artifacts to back up in WebCenter Portal enterprise deployments.

Table 16–1 Static Artifacts to Back Up in a WebCenter Portal (11g) Enterprise Deployment

Type	Host	Location	Tier
ORACLE HOME (DB)	RAC Database hosts - CUSTDBHOST1 and CUSTDBHOST2	The location is user-defined	Data Tier
ORACLE HOME (OHS)	WEBHOST1 and WEBHOST2	<code>ORACLE_BASE/admin/instance_name</code>	Web Tier
MW HOME (SOA + WC)	SOAHOST1 and SOAHOST2 - SOA WCPHOST1 and WCPHOST2 - WC	MW_HOME on all hosts	Application Tier

Table 16–1 (Cont.) Static Artifacts to Back Up in a WebCenter Portal (11g) Enterprise Deployment

Type	Host	Location	Tier
ORACLE HOME (WCC)	WCPHOST1 and WCPHOST2	On shared disk: /share/oracle/wcc On each host, local files at ORACLE_HOME/wcc	Application Tier
Installation-related files		OraInventory, user_home/boa/beahomelist, oraInst.loc, oratab	

Table 16–2 lists the runtime artifacts for back up in WebCenter Portal enterprise deployments.

Table 16–2 Run-Time Artifacts to Back Up in a WebCenter Portal (11g) Enterprise Deployment

Type	Host	Location	Tier
DOMAIN HOME	SOAHOST1 SOAHOST2 WCPHOST1 WCPHOST2	ORACLE_BASE/admin/domain_name/ mserver/domain_name	Application Tier
Application artifacts (ear and war files)	SOAHOST1 SOAHOST2 WCPHOST1 WCPHOST2	Look at all the deployments through admin console and back up all the application artifacts	Application Tier
OHS instance home	WEBHOST1 and WEBHOST2	ORACLE_BASE/admin/instance_name	Web Tier
OHS WCC configuration files	WEBHOST1 and WEBHOST2	On each host, at /share/oracle/wcc, which is a local file system.	Web Tier
RAC databases	CUSTDBHOST1 and CUSTDBHOST2	The location is user-defined	Data Tier
Oracle WebCenter Content repository		Database-based	Data Tier

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

16.7 Preventing Timeouts for SQLNet Connections

Much of the Enterprise Deployment production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall to not time out such connections. If such a configuration is not possible, set the `*SQLNET.EXPIRE_TIME=n*` parameter in the `sqlnet.ora` file, located in the following directory:

`ORACLE_HOME/network/admin`

The `n` indicates the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

16.8 Troubleshooting Oracle WebCenter Portal Enterprise Deployments

This section describes possible issues with WebCenter Portal enterprise deployment and suggested solutions.

This section covers the following topics:

- [Section 16.8.1, "Error While Activating Changes in Administration Console"](#)
- [Section 16.8.2, "Redirecting of Users to Login Screen After Activating Changes in Administration Console"](#)
- [Section 16.8.3, "Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM"](#)
- [Section 16.8.4, "WC_Spaces Server Does Not Start after Propagation of Domain"](#)
- [Section 16.8.5, "Administration Server Fails to Start After a Manual Failover"](#)
- [Section 16.8.6, "Portlet Unavailable After Database Failover"](#)
- [Section 16.8.7, "Configured JOC Port Already in Use"](#)
- [Section 16.8.8, "Restoring a JMS Configuration"](#)
- [Section 16.8.9, "OAM Configuration Tool Does Not Remove URLs"](#)
- [Section 16.8.10, "Disabling Secondary Authentication After REST Policy Configuration"](#)
- [Section 16.8.11, "Sudo Error Occurs During Server Migration"](#)

16.8.1 Error While Activating Changes in Administration Console

Problem: Activation of changes in Administration Console fails after changes to a server's start configuration have been performed. The Administration Console reports the following when clicking "Activate Changes":

An error occurred during activation of changes, please see the log for details.

```
[Management:141190]The commit phase of the configuration update failed with an exception:
```

```
In production mode, it's not allowed to set a clear text value to the property: PasswordEncrypted of ServerStartMBean
```

Solution: This may happen when start parameters are changed for a server in the Administration Console. In this case, either provide username/password information in the server start configuration in the Administration Console for the specific server whose configuration was being changed, or remove the `<password-encrypted></password-encrypted>` entry in the `config.xml` file (this requires a restart of the Administration Server).

16.8.2 Redirecting of Users to Login Screen After Activating Changes in Administration Console

Problem: After configuring OHS and load balancer to access the Oracle WebLogic Administration Console, some activation changes cause the redirection to the login screen for the admin console.

Solution: This is the result of the console attempting to follow changes to port, channel, and security settings as a user makes these changes. For certain changes, the console may redirect 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 `wcp.mycompany.com/console/console.portal` and directly access the home page for the Administration Console.

Note: This problem does not occur if you disabled tracking of the changes described in this section.

16.8.3 Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM

Problem: After configuring OAM, some activation changes cause the redirection to the Administration Console's home page (instead of the context menu where the activation was performed).

Solution: This is expected when OAM SSO is configured and is the result of the redirections performed by the Administration Server. Activation is completed regardless of the redirection. If required, users may "manually" navigate again to the desired context menu.

16.8.4 WC_Spaces Server Does Not Start after Propagation of Domain

Problem: WC_Spaces server fails to start after propagation the domain configuration to SOAHOST2, WCPHOST1 and WCPHOST2 using the `unpack` utility:

```
[Deployer:149158]No application files exist at '/u01/app/oracle/admin/wcpedg_domain/apps/wcpedg_domain/custom.webcenter.spaces.fwk'...
```

Solution: Copy all the files from the managed server applications location to the one expected by the managed server deployer. For example:

```
cp /u01/app/oracle/admin/wcpedg_domain/mserver/apps/*
/u01/app/oracle/admin/wcpedg_domain/apps/wcpedg_domain/
```

Note: Make sure `/u01/app/oracle/admin/wcpedg_domain/apps/wcpedg_domain/` exists before copying the contents.

16.8.5 Administration Server Fails to Start After a Manual Failover

Problem: Administration Server fails to start after the Administration Server node failed and manual failover to another nodes is performed. The Administration Server output log reports the following:

```
<Warning> <EmbeddedLDAP> <BEA-171520> <Could not obtain an exclusive lock for
directory:
ORACLE_BASE/admin/soadomain/aserver/
```



```
soadomain/servers/AdminServer/data/ldap/ldapfiles.
```

Waiting for 10 seconds and then retrying in case existing WebLogic Server is still shutting down.>

Solution: When restoring a node after a node crash and using shared storage for the domain directory, you may see this error in the log for the Administration Server due to unsuccessful lock cleanup. To resolve this error, remove the file:

```
ORACLE_BASE/ admin/domain_name/aserver/domain_
name/servers/AdminServer/data/ldap/ldapfiles/EmbeddedLDAP.lock
```

16.8.6 Portlet Unavailable After Database Failover

Problem: While creating a page inside the Spaces application, if you add a portlet to the page and a database failover occurs, an error component displays on the page:

```
"Error"
"Portlet unavailable"
```

This message remains even if you refresh the page or log out and back in again.

Solution: To resolve this issue, delete the component and add it again.

16.8.7 Configured JOC Port Already in Use

Problem: Attempts to start a Managed Server that uses the Java Object Cache, such as OWSM or WebCenter Portal Managed Servers, fail. The following errors appear in the logs:

```
J2EE JOC-058 distributed cache initialization failure
J2EE JOC-043 base exception:
J2EE JOC-803 unexpected EOF during read.
```

Solution: Another process is using the same port that JOC is attempting to obtain. Either stop that process, or reconfigure JOC for this cluster to use another port in the recommended port range.

16.8.8 Restoring a JMS Configuration

Problem: A mistake in the parameters passed to the `soa-createUDD.py` script, or some other mistake causes the JMS configuration for SOA clusters to fail.

Solution: Use `soa-createUDD.py` to restore the configuration.

If a mistake is made while running the `soa-createUDD.py` script after the SOA cluster is created from the Oracle Fusion Middleware Configuration Wizard (an incorrect option is used, a target is modified, or a module is deleted accidentally). In these situations you can use the `soa-createUDD.py` script to restore the appropriate JMS configuration using the following steps:

1. Delete the existing SOA JMS resources (JMS Modules owned by the `soa-infrastructure` system).
2. Run the `soa-createUDD.py` again. The script assume the JMS Servers created for SOA are preserved and creates the destinations and subdeployment modules required to use Uniform Distributed Destinations for SOA. In this case, the script should be executed with the option `--soacluster`. After running the script again, verified from the WebLogic Server Administration Console that the following artifacts exist (**Domain Structure, Services, Messaging, JMS Modules**):

```
SOAJMSModuleUDDs      ---->SOAJMSSubDM targeted to SOAJMSServer_auto_1 and
```

```
SOAJMSServer_auto_2
UMSJMSSystemResource ---->UMSJMSSubDMSOA targeted to UMSJMSServer_auto_1 and
UMSJMSServer_auto_2
```

16.8.9 OAM Configuration Tool Does Not Remove URLs

Problem: The OAM Configuration Tool has been used and a set of URLs were added to the policies in Oracle Access Manager. One or more URLs are incorrect. Executing the OAM Configuration Tool again with the correct URLs completes successfully; however, when accessing Policy Manager, the incorrect URL is still there.

Solution: The OAM Configuration Tool only adds new URLs to existing policies when executed with the same app_domain name. To remove a URL, use the Policy Manager Console in OAM. Log on to the Access Administration site for OAM, click **My Policy Domains**, click the created policy domain (WCP_EDG), then the **Resources** tab, and remove the incorrect URLs.

16.8.10 Disabling Secondary Authentication After REST Policy Configuration

Problem: After REST policy configuration, external clients authenticating through OAM are still prompted for further authentication.

Solution: The secondary authentication is coming from WebLogic. To disable the WebLogic credential prompt, you must update the security policy:

1. Locate the file:

```
/aserver/domain_name/config/config.xml
```

2. At the end of the security configuration section (that is, before `</security-configuration>`), add the line:

```
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-credentials>
```

3. Restart all the servers in the domain.

16.8.11 Sudo Error Occurs During Server Migration

Problem: When running `wlsifconfig` for server migration, the following warning displays:

```
sudo: sorry, you must have a tty to run sudo
```

Solution: The WebLogic user ('oracle') is not allowed to run sudo in the background. To solve this, add the following line into `/etc/sudoers`:

```
Defaults:oracle !requiretty
```

See also, [Section 14.6, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"](#).

Index

A

access gate, 15-19
adding clusters, 9-6, 10-5
adding managed servers, 9-6, 10-5
adding managed servers to existing nodes, 16-3
adding managed servers to new nodes, 16-9
address security filter, 13-22
Administration Console
 frontend URL, 8-19
 redirecting to home page, 16-20, 16-21
 redirecting to login screen, 16-20
 server migration verification, 14-7
administration server, 8-8, 8-10, 8-16, 14-3
 failover, 8-20, 8-22
 host name verification, 8-11, 8-13
 restarting, 13-21
 SSL communication, 11-2, 11-6
 starting, 8-9
 validating, 8-10
administrator role for WebCenter Portal
 Spaces, 15-42
admin.mycompany.com, 3-2
application tier, 2-4
arping, 8-2
ASM, see 'Automatic Storage Management (ASM)'
assigning servers to clusters, 9-6, 10-5
assigning servers to machines, 9-7, 10-6
associating Oracle web tier with WebLogic
 domain, 7-3
authenticators, 15-26, 15-39, 15-45
Automatic Storage Management (ASM), 5-2

B

backups
 after setting up Oracle HTTP Server, 6-3
 configuration files, 15-4, 15-27, 15-39
 Content Server, 13-12, 13-14
 database, 5-6
 domain, 9-3, 10-2
 enterprise deployments, 16-17
 installation, 6-9, 8-23, 9-24, 10-22, 15-46
 Oracle HTTP Server, 6-3
best practices
 timeouts for SQLNet connections, 16-18

boot.properties, 8-8
BPEL authentication, 15-45
BPMWorkflowAdmin application role, 15-45
built-in security, 1-5

C

cache for Java objects, 10-13
callback URL, 9-18
cluster agent, 1-3
clusters, 1-2, 8-6
 adding, 9-6, 10-5
 assigning servers, 9-6, 10-5
clusterware, 1-3
Coherence, see 'Oracle Coherence'
configuration
 database, 5-1
 delegated form authentication, 15-22
 directory structure, 4-1
 discussions server, 12-1
 domain on SOAHOST1, 8-3
 frontend HTTP host and port, 9-17
 high availability for Oracle File and FTP
 Adapters, 9-20
 Instant Messaging and Presence (IMP), 12-3
 load balancer, 3-2
 network, 3-1
 Oracle Coherence, 9-8
 Oracle HTTP Server, 7-3, 8-16
 Oracle HTTP Server for WLS managed
 servers, 9-15, 10-18
 pagelet producers, 12-6
 persistence store for transaction recovery, 9-19
 portlet producers, 12-5
 propagating domain configuration, 13-20
 scaling Oracle Database Adapter, 9-23
 shared JMS persistence store, 9-6
 shared storage, 4-1, 4-10
 targets for server migration, 14-5
 UMS drivers, 16-3
 use of custom keystores, 11-5, 11-8
 WebCenter Portal applications for OAM, 15-42
 WebGate, 15-22
 Workflow, 12-3
 Worklist, 12-3
Configuration Wizard, 8-3, 9-3, 10-3

- Configure JDBC Component Schema screen, 9-4
- Configure RAC Multi Data Source Component
 - Schema screen, 9-4
- configure-joc.py script, 8-15, 10-13
- connection factory parameters, 9-21
- connections
 - discussions server, 12-1
 - Instant Messaging and Presence (IMP), 12-3
 - Workflow, 12-3
 - Worklist, 12-3
- Content Server, 2-4
 - backup, 13-12, 13-14
- CREATE_SERVICE, 5-3
- createCentralInventory.sh script, 6-3, 6-5
- creating identity keystore, 11-3, 11-7
- creating trust keystore, 11-4
- CUSTDBHOST nodes, 2-5, 5-2
- custom keystores, 11-5, 11-8

D

- data sources, 8-5, 14-2
- data tier, 2-5
- database
 - backing up, 5-6
 - CREATE_SERVICE, 5-3
 - host requirements, 5-2
 - initialization parameters, 5-2
 - loading repository, 5-4
 - mutex locking, 9-20
 - services, 5-3
 - setting up, 5-1
 - supported versions, 5-2
- database listener port, 2-5
- database preconfiguration, 5-1
- default persistence store for transaction recovery, 9-19
- delegated form authentication, 15-22
- directory structure, 4-1, 4-2, 4-3, 4-8
- disabling host name verification, 8-11, 8-13, 9-11, 10-8
- discussions server, 12-1
- DMZ, 1-5, 2-3, 2-4
- domain
 - backing up, 9-3, 10-2
 - creating on SOAHOST1, 8-3
 - extending for SOA components, 9-1, 9-3
 - extending for WebCenter Portal components, 10-1, 10-2
 - propagating domain configuration, 13-20
- domain configuration
 - propagating, 8-13, 9-12, 9-14, 10-9, 10-10
- DOMAIN directory, 4-2
- domain directory, 8-10

E

- enabling ADMINVHN on SOAHOST1, 8-2
- enterprise deployment, 1-1
 - backups and recoveries, 16-17

- topology, 2-1
- environment privileges, 14-5
- extending domain
 - for SOA components, 9-1, 9-3
 - for WebCenter Portal components, 10-1, 10-2
- extending domain, WebCenter Content components, 13-1
- external communication, 1-5
- external services
 - discussions server, 12-1
 - Instant Messaging and Presence (IMP), 12-3
 - pagelet producers, 12-6
 - portlet producers, 12-5
 - Worklist, 12-3
- EXTRA_JAVA_PROPERTIES, 15-42

F

- failback, 1-2
- failover, 1-2, 16-20
- failover of administration server, 8-20, 8-22
- firewalls, 3-5
- frontend HTTP host and port, 9-17
- frontend URL for Administration Console, 8-19
- Fusion Middleware, see 'Oracle Fusion Middleware'

G

- generating self-signed certificates, 11-2, 11-6
- granting the Spaces administrator role, 15-42
- grid servers, 1-1

H

- hardware cluster, 1-2
- hardware requirements, 2-6
- high availability, 1-1, 1-6, 9-9
 - Oracle File and FTP Adapters, 9-20
- home page, redirecting to, 16-20, 16-21
- host identifier, 15-19
- host name, 9-9
 - network, 1-3
 - physical, 1-3
 - virtual, 1-4
- host name verification, 8-11, 8-13, 9-11, 10-8
- HTTP port, 2-3
- httpd.conf, 7-3
- HTTPS port, 2-3

I

- ID Asserter, 15-27, 15-39
- identity keystore, 11-3, 11-7
- ifconfig, 8-2
- IMP, see 'Instant Messaging and Presence (IMP)'
- Inbound Refinery
 - configuring, 13-21
 - extending the domain, 13-18
 - starting, 13-21
- incorrect URLs, 16-22
- initialization parameters for database, 5-2

installation
Oracle Fusion Middleware, 6-7
Oracle Fusion Middleware components, 6-5
Oracle Fusion Middleware Home, 6-3
Oracle HTTP Server, 6-2
Oracle WebCenter Content, 6-5
Oracle WebLogic Server, 6-4
procedure, 2-7
strategies, 2-10
validating web tier, 7-3
WebGate, 15-22
what to install, 2-6
Instant Messaging and Presence (IMP), 12-3
IPs, 3-4, 3-5

J

Java object cache, 10-13
JDBC component schema, 9-4
JDK, 6-5
JMS persistence store, 9-6
JRockit, 6-5

K

keystores
custom, 11-5, 11-8
identity, 11-3, 11-7
trust, 11-4
keytool utility, 11-4

L

LDAP
moving WebLogic administrator to --, 15-5
leading.ddl script, 14-2
leasing table for server migration, 14-1
listen address
WLS_WCC managed servers, 13-19
listen port
WLS_WCC managed servers, 13-19
load balancer, 2-3, 7-3
configuration, 3-2
configuring with Oracle HTTP Server, 7-3
requirements, 2-3
validating access, 10-22
locations of directories, 4-2, 4-3, 4-8
login screen, redirecting to, 16-20

M

managed servers, 8-6, 8-10
adding, 9-6, 10-5
adding to existing nodes, 16-3
adding to new nodes, 16-9
propagating domain changes, 9-12, 10-9
validation, 9-13, 9-14
WC_Collaboration, 10-11, 10-12, 10-18
WC_Portlet, 10-11, 10-12, 10-18
WC_Spaces, 10-11, 10-12, 10-18
WC_Uilities, 10-11, 10-12, 10-18

WebCenter Portal, 10-8
WLS_SOA, 9-11, 9-13, 9-14
WLS_WCC, 13-19
WLS_WSM, 8-8, 8-11, 8-12, 8-13, 8-14, 8-16
managing the topology, 16-1
manual failover, 16-20
manual failover of administration server, 8-20
mapping of IPs and VIPs, 3-4, 3-5
Middleware home, 1-2
migration of servers, see also 'server migration', 14-1
mod_wl_ohs.conf file, 8-17
monitoring the topology, 16-1
multi-data source, 14-2
mutex locking, 9-20
MW_HOME, 4-1

N

names of virtual servers, 3-1
network
firewalls, 3-5
IPs, 3-4
load balancers, 3-2
ports, 3-5
shared storage, 4-7
virtual IPs (VIPs), 3-4
virtual servers, 3-1
network host name, 1-3
network preconfiguration, 3-1
Node Manager, 14-3
properties file, 14-4
restarting, 9-12
setup, 11-1
SSL communication, 11-2, 11-6
starting, 8-8, 8-14, 10-8, 10-10, 11-5, 11-8, 13-9
use of custom keystores, 11-5, 11-8
nodes
adding servers to existing --, 16-3
adding servers to news --, 16-9
application tier, 2-4
CUSTDBHOST, 2-5, 5-2
data tier, 2-5
primary, 1-3
secondary, 1-3
SOAHOST, 8-2, 8-3, 8-8, 8-14, 9-12, 10-8, 13-9
WCPHOST, 10-8, 10-10
web tier, 2-3
WEBHOST, 2-3, 6-2

O

OAM, see 'Oracle Access Manager (OAM)'
OAMCFG tool, 16-22
overview, 15-13
running, 15-13
OAP port, 2-5
OID authenticator, 15-4
OID ports, 2-5
OmniPortlet URL, 12-5

- Oracle Access Manager, 2-3
- Oracle Access Manager (OAM)
 - BPEL authentication, 15-45
 - configuring WebCenter Portal applications, 15-42
 - delegated form authentication, 15-22
 - ID Asserter, 15-27, 15-39
 - OAMCFG tool, 15-13
 - order of providers, 15-27, 15-40
 - overview, 15-12, 15-29
 - prerequisites, 15-12, 15-30
 - updating host identifier, 15-19
 - updating WebGate profile, 15-20
 - verifying access gate, 15-19
 - verifying policy domain, 15-18
 - WebGate, 15-22
 - WebLogic authenticators, 15-26, 15-39
- Oracle Access Protocol (OAP), 2-3
- Oracle Coherence, 9-8
 - specifying host name, 9-9
- Oracle Database Adapter, scaling, 9-23
- Oracle File and FTP Adapters, 9-20
- Oracle Fusion Middleware
 - installation, 6-7
 - installing Home, 6-3
 - installing Oracle WebLogic Server, 6-4
- Oracle Fusion Middleware (FMW)
 - installing FMW components, 6-5
- Oracle Fusion Middleware Configuration Wizard, 8-3
- Oracle home, 1-2
- Oracle HTTP Server
 - backup, 6-3
 - configuration, 8-16
 - configuration for WLS managed servers, 10-18
 - installation, 6-2
 - registering, 8-19
 - validating access, 8-20, 8-22, 9-17, 10-21
 - validation, 7-3
- Oracle HTTP Server (OHS)
 - backing up, 6-3
 - configuration, 7-3
 - load balancer, 7-3
 - port, 6-2
- Oracle instance, 1-2
- Oracle SOA Suite
 - installation, 6-5
- Oracle WebCenter Content, 2-4
 - ports, 3-7, 3-8
- Oracle WebCenter Portal
 - configuring Analytics, 10-16
 - configuring Collector clusters, 10-16
 - configuring the WC_Spaces servers, 10-16
- Oracle WebLogic Server
 - installation, 6-4
 - registering Oracle HTTP Server, 8-19
- Oracle WebLogic Server (WLS)
 - associating with Oracle web tier, 7-3
- Oracle WebLogic Server Administration Console, 14-2
- ORACLE_BASE, 4-1

- ORACLE_HOME, 4-2
- ORACLE_INSTANCE, 4-2
- oracleRoot.sh script, 6-3

P

- pagelet producers, 12-6
- parameters for connection factory, 9-21
- performance, enterprise deployment and, 1-1
- persistence store
 - shared JMS, 9-6
 - transaction recovery, 9-19
- physical host name, 1-3
- physical IP, 1-4
- policy domain, 15-18
- portlet producers, 12-5
- portlets, 16-21
- ports
 - database listener, 2-5
 - frontend HTTP, 9-17
 - HTTP, 2-3
 - HTTPS, 2-3
 - Oracle HTTP Server, 6-2
 - Oracle Internet Directory (OID), 2-5
 - Oracle WebCenter Content, 3-7, 3-8
 - used in topology, 3-5
- preconfiguration
 - database, 5-1
 - directory structure, 4-1
 - network, 3-1
 - shared storage, 4-1
- primary node, 1-3
- PROCESSES parameter for database, 5-3
- propagating domain changes, 9-12, 10-9
- propagating domain configuration, 8-13, 9-14, 10-10, 13-20
- properties file of Node Manager, 14-4
- provider order for OAM, 15-27, 15-40

R

- RAC database, 2-5, 8-5
- RAC multi-data source component schema, 9-4
- recovery of enterprise deployments, 16-17
- redirecting to home page, 16-20, 16-21
- redirecting to login screen, 16-20
- reference topology, 2-1
- registering Oracle HTTP Server, 8-19
- registering pagelet producers, 12-6
- registering portlet producers, 12-5
- Repository Creation Utility (RCU), 5-1, 5-4
- requirements
 - database host, 5-2
 - load balancer, 2-3
- requirements, hardware, 2-6
- restarting
 - administration server, 13-21
 - restarting Node Manager, 9-12

S

- scaling Oracle Database Adapter, 9-23
- scaling out the topology, 16-9
- scaling up the topology, 16-3
- screens
 - Configure JDBC Component Schema, 9-4
 - Configure RAC Multi Data Source Component Schema, 9-4
- scripts
 - configure-joc.py, 8-15, 10-13
 - createCentralInventory.sh, 6-3, 6-5
 - leasing.ddl, 14-2
 - oracleRoot.sh, 6-3
 - setDomainEnv.sh, 15-42
 - setNMProps.sh, 8-8, 8-14
 - wlsifconfig.sh, 14-5
- secondary node, 1-3
- security, 1-5
- security filter, 13-22
- self-signed certificates, 11-2, 11-6
- server migration, 14-1
 - configuring targets, 14-5
 - creating a multi-data source, 14-2
 - editing Node Manager's properties file, 14-4
 - enabling SSL communication, 14-3
 - leasing table, 14-1
 - multi-data source, 14-2
 - setting environment and superuser privileges, 14-5
 - setting up user and tablespace, 14-1
 - testing, 14-6
 - verification from Administration Console, 14-7
- servers, 8-6
 - assigning to clusters, 9-6, 10-5
 - assigning to machines, 9-7, 10-6
- service level agreements, 1-1
- setDomainEnv.sh script, 15-42
- setNMProps.sh script, 8-8, 8-14
- setting up Java object cache, 10-13
- setting up Node Manager, 11-1
- setting up WebLogic authenticators, 15-26, 15-39
- shared JMS persistence store, 9-6
- shared storage, 1-3, 4-1, 4-7
 - configuration, 4-10
- SOAHOST nodes, 8-2, 8-3, 8-8, 8-14, 9-12, 10-8, 13-9
 - installing Oracle SOA Suite, 6-5
- SOAHOST1VHn virtual hosts, 9-9
- Spaces
 - discussions server, 12-1
- SQLNet connections, timeouts, 16-18
- SSL acceleration, 2-4
- SSL communication, 11-2, 11-6, 14-3
- SSO mode, 15-42
- starting administration server, 8-9
- starting Node Manager, 8-8, 8-14, 10-8, 10-10, 11-5, 11-8, 13-9
- starting WC_Collaboration managed server, 10-11, 10-12
- starting WC_Portlet managed server, 10-11, 10-12
- starting WC_Spaces managed server, 10-11, 10-12

- starting WC_Utilities managed server, 10-11, 10-12
- starting WLS_SOA managed server, 9-13, 9-14
- starting WLS_WSM managed server, 8-12, 8-14
- storage, 4-1, 4-7
- strategies for installation, 2-10
- superuser privileges, 14-5
- supported database versions, 5-2
- switchback, 1-4
- switchover, 1-4

T

- targeted applications, 9-7
- targeting deployments, 8-7
- targets for server migration, 14-5
- testing of server migration, 14-6
- timeouts for SQLNet connections, 16-18
- topology, 2-1
 - application tier, 2-4
 - data tier, 2-5
 - database, 5-1
 - directory structure, 4-1
 - managing, 16-1
 - monitoring, 16-1
 - network, 3-1
 - scaling out, 16-9
 - scaling up, 16-3
 - shared storage, 4-1
 - web tier, 2-3
- transaction recovery, 9-19
- troubleshooting
 - activating changes in Admin Server, 16-19
 - incorrect URLs, 16-22
 - manual failover, 16-20
 - portlet unavailable, 16-21
 - redirecting to home page, 16-20, 16-21
 - redirecting to login screen, 16-20
- trust keystore, 11-4

U

- UMS drivers, 16-3
- unicast communication, 2-5, 9-8
- unpack utility, 8-13, 9-14, 10-10
- updating the host identifier, 15-19
- updating WebGate profile, 15-20
- URL, callback, 9-18
- utils.CertGen utility, 11-2, 11-6
- utils.ImportPrivateKey utility, 11-3, 11-7

V

- validation
 - access through load balancer, 10-22
 - access through Oracle HTTP Server, 8-20, 8-22, 9-17, 10-21
 - administration server, 8-10
 - Oracle HTTP Server, 7-3
 - server migration, 14-6
 - WC_Collaboration managed server, 10-11, 10-12
 - WC_Portlet managed server, 10-11, 10-12

- WC_Spaces managed server, 10-11, 10-12
- WC_Uilities managed server, 10-11, 10-12
- web tier installation, 7-3
- WLS_SOA managed server, 9-13, 9-14
- WLS_WSM managed server, 8-12, 8-14, 9-13
- verification of host names, 8-11, 8-13, 9-11, 10-8
- VIPs, 3-4, 3-5
 - enabling ADMINVHN on SOAHOST1, 8-2
- virtual host name, 1-4
- virtual IP, 1-4
- virtual IPs (VIPs), 3-4, 3-5
- virtual server names, 3-1
- virtual servers, 2-3
 - admin.mycompany.com, 3-2
 - wcpinternal.mycompany.com, 3-2
 - wcp.mycompany.com, 3-2
- <VirtualHost> entries in httpd.conf, 7-3

- Workflow, 12-4
- Worklist, 12-4
- WebLogic Server home, 1-2
- WebLogic Server, see 'Oracle WebLogic Server'
- WL_HOME, 4-1
- WLS_SOA
 - disabling host name verification, 9-11
- WLS_WCC managed servers, 13-19
- WLS_WSM, 8-8, 8-16
 - disabling host name verification, 8-11, 8-13
 - starting, 8-12, 8-14
 - validating, 8-12, 8-14
- wlsifconfig.sh script, 14-5
- WLST, see 'WebLogic Scripting Tool'
- Workflow, 12-3
- Worklist, 12-3

W

- WC_Collaboration managed server, 10-11, 10-12, 10-18
- WC_Portlet managed server, 10-11, 10-12, 10-18
- WC_Spaces managed server, 10-11, 10-12, 10-18
- WC_Uilities managed server, 10-11, 10-12, 10-18
- WCPHOST
 - propagating domain configuration, 13-20
- WCPHOST nodes, 10-8, 10-10
- wcpinternal.mycompany.com, 3-2
- wcp.mycompany.com, 3-2
- web tier, 2-3
 - associating with WebLogic domain, 7-3
 - validating installation, 7-3
- WebCenter Portal
 - authentication, 15-45
 - configuring applications for OAM, 15-42
 - disabling host name verification, 10-8
 - extending domain for --, 10-1, 10-2
 - installing Oracle Fusion Middleware, 6-7
- WebCenter Portal Spaces
 - administrator role, 15-42
 - Java object cache, 10-13
 - portlet producers, 12-5
 - SSO mode, 15-42
 - Workflow, 12-3
 - Worklist, 12-3
- WebClipping URL, 12-5
- WebGate, 2-3, 15-22
- WebGate profile, 15-20
- WEBHOST
 - associating web tier with WebLogic domain, 7-3
 - configuring OHS with load balancer, 7-3
 - configuring web tier, 7-1
- WEBHOST nodes, 2-3, 6-2
- WebLogic administrator, moving to LDAP, 15-5
- WebLogic authenticators, 15-26, 15-39
- WebLogic Configuration Wizard, 8-3
- WebLogic Scripting Tool (WLST)
 - discussions server, 12-2
 - portlet producers, 12-5