Oracle® Fusion Middleware
Enterprise Deployment Guide for Oracle WebCenter Content
11g Release 1 (11.1.1)
E15483-08

September 2012
Documentation for installers that describes how to install and configure Oracle WebCenter Content components in an enterprise deployment. Includes best practices blueprint for an Oracle WebCenter Content enterprise deployment topology.
Preface
Audience
Documentation Accessibility
Related Documents
Conventions

1 Enterprise Deployment Overview
1.1 About the Enterprise Deployment Guide
1.2 About Oracle WebCenter Content
1.3 Enterprise Deployment Terminology
1.4 Benefits of Oracle Recommendations
   1.4.1 Built-In Security
   1.4.2 High Availability

2 Introduction to the Enterprise Deployment Reference Topology
2.1 Overview of the Enterprise Deployment Reference Topology
   2.1.1 Reference Topology Documented in the Guide
   2.1.2 About Oracle Identity Management Integration
   2.1.3 About the Web Tier Nodes
   2.1.4 About the Application Tier
   2.1.5 About the Data Tier
   2.1.6 About the Unicast Requirement for Communication
2.2 Hardware Requirements for an Enterprise Deployment on Linux
2.3 Clock Synchronization
2.4 Identifying the Software Components to Install
2.5 Roadmap for the Reference Topology Installation and Configuration
   2.5.1 Flow Chart of the Oracle WebCenter Content Enterprise Deployment Process
   2.5.2 Steps in the Oracle WebCenter Content Enterprise Deployment Process
   2.5.3 Understanding the Incremental, Modular Approach to Enterprise Deployment

3 Preparing the Network for an Enterprise Deployment
3.1 Overview of Preparing the Network for an Enterprise Deployment
3.2 Virtual Server Names Used by the Topology
   3.2.1 wcc.mycompany.com
   3.2.2 admin.mycompany.com
8 Creating a Domain for an Enterprise Deployment

8.1 Overview of Creating a Domain .......................................................... 8-1
8.2 Enabling ADMINVHN on SOAHOST1 ............................................. 8-2
8.3 Running the Configuration Wizard on SOAHOST1 to Create a Domain ........................................................................ 8-3
8.4 Post-Configuration and Verification Tasks .................................. 8-5
8.4.1 Verifying the RAC Database Service ........................................ 8-5
8.4.2 Creating boot.properties for the Administration Server on SOAHOST1 .......................................................... 8-5
8.4.3 Starting Node Manager on SOAHOST1 .................................. 8-6
8.4.4 Starting the Administration Server on SOAHOST1 ............ 8-7
8.4.5 Validating the Administration Server Configuration .................. 8-8
8.4.6 Disabling Host Name Verification for the Administration Server .......................................................... 8-8
8.5 Configuring Oracle HTTP Server for the WebLogic Domain .......... 8-9
8.5.1 Configuring Oracle HTTP Server for the Administration Server .......................................................... 8-9
8.5.2 Turning on the WebLogic Plug-In enabled Flag .................. 8-10
8.5.3 Registering Oracle HTTP Server with WebLogic Server ........... 8-10
8.5.4 Setting the Frontend URL for the Administration Console and Setting Redirection Preferences ........................................................................ 8-11
8.5.5 Validating Access Through Oracle HTTP Server .................. 8-11
8.5.6 Verifying Manual Failover of the Administration Server .......................................................... 8-12
8.5.6.1 Assumptions and Procedure .......................................................... 8-13
8.5.6.2 Validating Access to SOAHOST2 Through Oracle HTTP Server ........................................................................ 8-14
8.5.6.3 Failing the Administration Server Back to SOAHOST1 .......... 8-14
8.6 Backing Up the WebLogic Server Domain Configuration .......... 8-14

9 Extending the Domain to Include Oracle SOA Suite Components

9.1 Overview of Extending the Domain for Oracle SOA Suite Components .......................................................... 9-2
9.2 Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2 .... 9-3
9.3 Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard .......................................................... 9-3
9.4 Configuring Oracle Coherence for Deploying Composites .......................................................... 9-11
9.4.1 Enabling Communication for Deployment Using Unicast Communication .......................................................... 9-11
9.4.2 Specifying the Host Name .......................................................... 9-12
9.5 Completing Post-Configuration and Verification Tasks ............ 9-14
9.5.1 Disabling Host Name Verification for the WLS_SOAt Managed Servers .......................................................... 9-14
9.5.2 Restarting Node Manager on SOAHOST1 .................................. 9-15
9.5.3 Validating GridLink Data Sources .......................................................... 9-15
9.5.4 Propagating the Domain Changes to the Managed Server Domain Directory .......... 9-18
9.5.5 Starting and Validating the WLS_SOAt Managed Server .......................................................... 9-18
9.5.6 Propagating the Domain Configuration to SOAHOST2 .......... 9-19
9.5.6.1 Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility .......................................................... 9-19
9.5.6.2 Starting and Validating the WLS_SOAt Managed Server .......................................................... 9-20
9.6 Configuring the Java Object Cache for Oracle Web Services Manager ................................ 9-20
9.7 Configuring Oracle HTTP Server for the WLS_SOA Managed Servers .................................. 9-22
9.8 Setting the Frontend HTTP Host and Port ............................................................................. 9-24
9.9 Validating Access Through Oracle HTTP Server .................................................................. 9-25
9.10 Configuring a Default Persistence Store for Transaction Recovery ........................................ 9-25
9.11 Enabling High Availability for Oracle File and FTP Adapters ............................................. 9-26
9.12 Scaling the Oracle Database Adapter .................................................................................... 9-29
9.13 Configuring Node Manager for the WLS_SOA Managed Servers ........................................ 9-30
9.14 Configuring Server Migration for the WLS_SOA Managed Servers ...................................... 9-30
9.15 Backing Up the Installation .................................................................................................. 9-30

10 Extending the Domain to Include Oracle WebCenter Content
10.1 Overview of Extending the Domain to Include Oracle WebCenter Content ......................... 10-2
10.2 Enabling WCCHOST1VHN1 on WCCHOST1 and WCCHOST2VHN1 on WCCHOST2 ............................................................. 10-3
10.3 Extending the Domain to Include WebCenter Content .......................................................... 10-3
10.4 Starting Node Manager on WCCHOST1 and WCCHOST2 ....................................................... 10-14
10.5 Validating GridLink Data Sources for WCC_WLS1 .................................................................. 10-14
10.6 Propagating the Domain Configuration to the Managed Server Domain Directories .......... 10-17
10.7 Restarting the Administration Server ..................................................................................... 10-17
10.8 Starting the WLS_WCC1 Managed Server and Configuring Content Server .......................... 10-18
10.9 Updating the cwallet File in the Administration Server ........................................................ 10-19
10.10 Starting the WLS_WCC2 Managed Server and Configuring Content Server ....................... 10-19
10.11 Validating GridLink Data Sources for WLS_WCC2 .............................................................. 10-21
10.12 Configuring Service Retries for Oracle WebCenter Content ............................................. 10-21
10.13 Configuring Oracle HTTP Server for the WLS_WCC Managed Servers .............................. 10-22
10.14 Validating Access Through Oracle HTTP Server ................................................................ 10-22
10.15 Configuring Node Manager for the WLS_WCC and WLS_IMG Managed Servers .......... 10-23
10.16 Backing Up the Installation ................................................................................................. 10-24

11 Extending the Domain to Include Imaging
11.1 Overview of Extending the Domain for Imaging ................................................................. 11-2
11.2 Enabling VIP4 and VIP5 in WCCHOST1and WCCHOST2 ...................................................... 11-4
11.3 Extending the Domain to Include Imaging .......................................................................... 11-4
11.4 Disabling Host Name Verification for the WLS_IMG Managed Servers ............................... 11-11
11.5 Starting Node Manager on WCCHOST1 and WCCHOST2 ................................................... 11-12
11.6 Validating GridLink Data Sources for WCC_IMG1 .............................................................. 11-12
11.7 Propagating the Domain Configuration to the Managed Server Domain Directories .......... 11-15
11.8 Configuring a JMS Persistence Store for Oracle WebCenter Content: Imaging ................ 11-15
11.9 Configuring a Default Persistence Store for Transaction Recovery .................................... 11-16
11.10 Restarting the Administration Server .................................................................................. 11-17
11.11 Starting the Imaging Managed Servers ............................................................................... 11-17
11.12 Validating GridLink Data Sources for WLS_IMG2 .............................................................. 11-18
11.13 Configuring System MBeans for Oracle WebCenter Content: Imaging .............................. 11-18
11.14 Enabling the Imaging Feature Set in Oracle WebCenter Content ...................................... 11-20
11.15 Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content ........................................................................................................ 11-20
11.16 Creating a Connection to Oracle WebCenter Content ................................................... 11-20
11.17 Configuring BPEL CSF Credentials .................................................................................. 11-21
11.18 Configuring a Workflow Connection ............................................................................... 11-22
11.19 Configuring Oracle HTTP Server for the WLS_IMG Managed Servers ....................... 11-23
11.20 Setting the Frontend HTTP Host and Port ..................................................................... 11-23
11.21 Validating Access Through Oracle HTTP Server .......................................................... 11-24
11.22 Configuring Node Manager for the WLS_IMG Managed Servers .................................. 11-24
11.23 Configuring Server Migration for the WLS_IMG Managed Servers ............................... 11-24
11.24 Backing Up the Installation .............................................................................................. 11-25

12 Extending the Domain to Include Inbound Refinery
12.1 Overview of Extending the Domain for Oracle WebCenter Content: Inbound Refinery ................................................................................................................................. 12-1
12.2 Associating Inbound Refinery Managed Servers with Virtual Host Names ..................... 12-2
12.3 Extending the Domain to Include Inbound Refinery ........................................................ 12-3
12.4 Starting Node Manager on WCCHOST1 and WCCHOST2 .............................................. 12-8
12.5 Propagating the Domain Configuration to the Managed Server Domain Directories .. 12-8
12.6 Restarting the Administration Server ............................................................................... 12-9
12.7 Starting the Inbound Refinery Managed Servers ............................................................. 12-9
12.8 Configuring the Inbound Refineries .................................................................................. 12-9
12.8.1 Configuring Inbound Refinery Settings ...................................................................... 12-10
12.8.2 Configuring Document Conversion ............................................................................ 12-11
12.8.3 Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion ............ 12-12
12.8.3.1 Creating an Outgoing Provider .............................................................................. 12-12
12.8.3.2 Enabling Components for Inbound Refinery on Content Server ......................... 12-13
12.8.3.3 Selecting File Formats To Be Converted .............................................................. 12-13
12.9 Validating the Configuration of the Inbound Refinery Managed Servers ....................... 12-14

13 Setting Up Node Manager
13.1 Overview of Setting Up Node Manager ............................................................................ 13-1
13.2 Changing the Location of the Node Manager Log ............................................................ 13-2
13.3 Enabling Host Name Verification Certificates for Node Manager .................................... 13-2
13.3.1 Generating Self-Signed Certificates Using the utils.CertGen Utility .......................... 13-3
13.3.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility ..................... 13-4
13.3.3 Creating a Trust Keystore Using the Keytool Utility .................................................. 13-4
13.3.4 Configuring Node Manager to Use the Custom Keystores ........................................ 13-5
13.3.5 Configuring Managed Servers to Use the Custom Keystores .................................... 13-6
13.3.6 Changing the Host Name Verification Setting for the Managed Servers ................. 13-7
13.4 Starting Node Manager ..................................................................................................... 13-7

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 ................. 14-2
14.3 Creating a GridLink Data Source for Leasing Using the Administration Console ............ 14-3
14.4 Enabling Host Name Verification Certificates between HOST1 and HOST2 and the Administration Server ................................................................. 14-5
15 Integrating with Oracle Identity Management

15.1 Overview of Integrating with Oracle Identity Management ........................................ 15-1
15.2 Credential and Policy Store Configuration ........................................................................ 15-2
15.2.1 Overview of Credential and Policy Store Configuration ........................................... 15-2
15.2.2 Credential Store Configuration ....................................................................................... 15-3
15.2.2.1 Creating the LDAP Authenticator .............................................................................. 15-3
15.2.2.2 Moving the WebLogic Server Administrator to LDAP ............................................. 15-4
15.2.2.3 Reassociating the Domain Credential Store ............................................................. 15-6
15.2.3 Policy Store Configuration .............................................................................................. 15-7
15.2.3.1 Prerequisites to Using an LDAP-Based Policy Store............................................... 15-7
15.2.3.2 Reassociating the Domain Policy Store ................................................................. 15-9
15.2.4 Reassociation of Credentials and Policies ................................................................. 15-10
15.2.4.1 Cataloging Oracle Internet Directory Attributes .................................................... 15-10
15.3 Oracle Access Manager 10g Integration ................................................................. 15-11
15.3.1 Overview of Oracle Access Manager Integration ..................................................... 15-11
15.3.2 Prerequisites for Oracle Access Manager ............................................................... 15-12
15.3.3 Configuring Oracle Access Manager .............................................................................. 15-13
15.3.3.1 Collecting the Information for the OAM Configuration Tool ................................ 15-13
15.3.3.2 Running the OAM Configuration Tool ................................................................. 15-14
15.3.3.3 Oracle Access Manager Logout Guidelines ............................................................ 15-15
15.3.3.4 Verifying Successful Creation of the Policy Domain and AccessGate ................ 15-16
15.3.3.5 Verifying That the Cookieless Basic Authorization Scheme Has Been Properly Assigned ................................................................. 15-16
15.3.3.6 Updating the Host Identifier ..................................................................................... 15-17
15.3.3.7 Updating the WebGate Profile ................................................................................. 15-18
15.3.3.8 Adding Additional Access Servers .......................................................................... 15-19
15.3.3.9 Configuring Delegated Form Authentication .......................................................... 15-19
15.3.4 Installing and Configuring WebGate ........................................................................... 15-20
15.3.5 Configuring IP Validation for the Enterprise Deployment Webgate ........................ 15-24
15.3.6 Setting Up WebLogic Server Authenticators .............................................................. 15-25
15.3.6.1 Back Up Configuration Files ................................................................................... 15-25
15.3.6.2 Setting Up the Oracle Access Manager Identity Asserter ......................................... 15-25
15.3.6.3 Setting the Order of Providers ................................................................................ 15-25
15.3.7 Oracle Access Manager 11g Integration ..................................................................... 15-26
15.4.1 Overview of Oracle Access Manager Integration ..................................................... 15-26
15.4.2 Prerequisites for Oracle Access Manager ............................................................... 15-26
15.4.3 Setting Up WebGate ................................................................................................. 15-27
15.4.3.1 Installing GCC Libraries ......................................................................................... 15-27
15.4.3.2 Installing WebGate ............................................................................................... 15-27
15.4.3.3 Post-Installation Steps ......................................................................................... 15-28
16 Managing the Topology

16.1 Overview of Managing the Oracle WebCenter Content Topology ................................................. 16-2
16.2 Defining an Optimal Input File Strategy for Oracle WebCenter Content: Imaging .......... 16-3
16.3 Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology .............................................................. 16-3
16.4 Managing Space in the SOA Infrastructure Database................................................................. 16-4
16.5 Configuring UMS Drivers for Oracle WebCenter Content: Imaging ................................. 16-4
16.6 Scaling Up the Oracle WebCenter Content Topology.............................................................. 16-5
16.6.1 Scale-Up Procedure for Oracle WebCenter Content ......................................................... 16-6
16.6.2 Scale-Up Procedure for Oracle WebCenter Content: Imaging ...................................... 16-6
16.6.3 Scale-Up Procedure for Oracle SOA Suite ........................................................................... 16-10
16.7 Scaling Out the Oracle WebCenter Content Topology ......................................................... 16-14
16.7.1 Scale-Out Procedure for Oracle WebCenter Content ....................................................... 16-15
16.7.2 Scale-Out Procedure for Oracle WebCenter Content: Imaging ...................................... 16-18
16.7.3 Scale-Out Procedure for Oracle SOA Suite ........................................................................ 16-23
16.8 Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments ........................................................................................................ 16-28
16.9 Preventing Timeouts for SQLNet Connections ........................................................................ 16-29
16.10 Configuring Oracle Web Service Manager Security Policies for Oracle WebCenter Content and Imaging Services ................................................................. 16-29
16.11 Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology .... 16-30
16.11.1 Page Not Found When Accessing soa-infra Application Through Load Balancer .................. 16-30
16.11.2 Soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence) ......................................................................................................................... 16-31
16.11.3 Incomplete Policy Migration After Failed Restart of SOA Server ........................................ 16-31
16.11.4 SOA, Oracle WebCenter Content, or Imaging Servers Fail to Start Due to Maximum Number of Processes Available in Database .................................................. 16-32
16.11.5 Administration Server Fails to Start After a Manual Failover ............................................... 16-33
16.11.6 Error While Activating Changes in Administration Console ............................................. 16-33
16.11.7 SOA or Imaging Server Not Failed Over After Server Migration ......................................... 16-33
16.11.8 SOA or Imaging Server Not Reachable From Browser After Server Migration........ 16-33
A Using Multi Data Sources with Oracle RAC

A.1 About Multi Data Sources and Oracle RAC .............................................. A-1
A.2 Typical Procedure for Configuring Multi Data Sources for an EDG Topology .... A-1

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

**Audience**

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

**Documentation Accessibility**

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

**Access to Oracle Support**

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

**Related Documents**

For more information, see the following documents:

- *Oracle WebCenter Content Quick Installation Guide*
- *Oracle WebCenter Content Installation Guide*
- *Oracle Fusion Middleware Administrator’s Guide*
Conventions

The following text conventions are used in this document.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
This chapter provides an overview of the enterprise deployment for Oracle WebCenter Content. It includes the following topics:

- Section 1.1, "About the Enterprise Deployment Guide"
- Section 1.2, "About Oracle WebCenter Content"
- Section 1.3, "Enterprise Deployment Terminology"
- Section 1.4, "Benefits of Oracle Recommendations"

### 1.1 About the Enterprise Deployment Guide

An enterprise deployment guide is an Oracle best practices blueprint based on proven Oracle high-availability and security technologies and recommendations for Oracle Fusion Middleware. The best practices described in these blueprints span all Oracle products across the entire technology stack: Oracle Database, Oracle Fusion Middleware, Oracle Applications, and Oracle Enterprise Manager Fusion Middleware Control.

An Oracle Fusion Middleware enterprise deployment does the following:

- 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


---

**Note:** This document focuses on enterprise deployments in Linux environments, but enterprise deployments can also be implemented in UNIX and Windows environments.
1.2 About Oracle WebCenter Content

The Oracle WebCenter Content suite (formerly known as Oracle Enterprise Content Management Suite, or Oracle ECM) provides unified content management that ensures seamless access to the right information in the appropriate business context by helping organizations implement a strategic content infrastructure for managing documents, images, and rich media files while delivering contextual integration with enterprise applications.

Oracle WebCenter Content provides the following key benefits:

- Reduce costs: lower printing, shipping, storage, and maintenance costs
- Gain efficiencies: with a single source of truth, streamlined business processes, and more complete and faster access to information.
- Reduce risk: improve consistency and auditable, comply with business policies and regulations, ensure content security, and better manage your brand
- Create value: improve business agility and optimize revenue by improving cross-selling and up-selling; enabling your channels; and improving customer retention.

The reference enterprise deployment topology in this guide includes the following Oracle WebCenter Content feature sets:

- Oracle WebCenter Content
- Oracle WebCenter Content: Imaging
- Oracle WebCenter Content: Inbound Refinery

Oracle WebCenter Content

Oracle WebCenter Content (formerly known as Oracle Universal Content Management, or Oracle UCM) provides organizations with a unified repository to house unstructured content, and deliver it to business users in the proper format, and within the context of familiar applications to fit the way they work.

Oracle WebCenter Content: Imaging

Oracle WebCenter Content: Imaging (formerly known as Oracle Imaging and Process Management, or Oracle I/PM) is the most complete, integrated, and cost-effective imaging platform for end-to-end management of document images within enterprise business processes. It leverages Oracle WebCenter Capture for image capture, Oracle WebCenter Forms Recognition for intelligent data capture, and provides annotation and markup of images, automates routing and approvals, and a scalable repository supporting enterprise-wide applications. With Imaging, organizations can quickly automate business processes in Oracle and other third-party enterprise applications.

Oracle WebCenter Content: Inbound Refinery

Oracle WebCenter Content: Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video. In addition to conversion, Inbound Refinery provides thumbnail functionality for documents and images, storyboarding for video, and the ability to extract and use EXIF data from digital images and XMP data from electronic files generated from programs such as Adobe Photoshop and Adobe Illustrator. Organizations can use Inbound Refinery to convert content items stored in Oracle WebCenter Content Server.
1.3 Enterprise Deployment Terminology

The following terminology is used in this enterprise deployment guide:

- **Oracle home**: An Oracle home contains installed files necessary to host a specific product. For example, the SOA Oracle home contains a directory that contains binary and library files for Oracle SOA Suite. 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**: The Oracle home that contains the binary and library files required for 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, and 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 handles the load by using the other available systems. 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 the *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, including Oracle, 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**: 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)

Except for a WebCenter Content or Inbound Refinery managed server, you can locate a managed server home on the shared disk as well. 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 and write to.

- **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 address of a machine on the network. In almost most 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.
1.4 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 1.4.1, "Built-In Security"
- Section 1.4.2, "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.

1.4.1 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.


- Communication from external clients does not go beyond the Load Balancing Router (LBR) 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.
- Oracle 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.

1.4.2 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.
This chapter describes and illustrates the enterprise deployment reference topology described in this guide. The roadmap for installation and configuration directs you to the appropriate chapters for the tasks you need to perform. Use this chapter to help you plan your Oracle WebCenter Content enterprise deployment.

This chapter includes these topics:

- Section 2.1, "Overview of the 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, "Roadmap for the Reference Topology Installation and Configuration"

2.1 Overview of the Enterprise Deployment Reference Topology

This section describes a diagram used to illustrate the enterprise deployment reference topology described in this guide. 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 service-oriented architecture (SOA) and Oracle WebCenter Content 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 Reference Topology for Oracle WebCenter Content


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 Server domain. The Oracle IDM enterprise deployment is separate from the Oracle WebCenter Content enterprise deployment and exists in a separate domain by itself. For more information on Oracle Identity Management in an enterprise deployment context, see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

The primary interface to the Oracle IDM enterprise deployment is the LDAP traffic to the LDAP servers, the OAP (Oracle Access Protocol) to the Oracle Access Manager 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.

**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 back-end 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 back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.

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 back-end 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.

### 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 Oracle WebLogic Server configured with managed servers for running Oracle SOA Suite components, such as BPEL Process Manager. The managed servers are configured in an active-active manner.

WCCHOST1 and WCCHOST2 run the Oracle WebCenter Content servers, Imaging servers, and Inbound Refinery servers.

SOAHOST1 and SOAHOST2 also 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 8.5.6, "Verifying Manual Failover of the Administration Server"). Alternatively, you can configure the WebLogic Server Administration Console with CFC/CRS to fail over automatically on a separate hardware cluster (not shown in this architecture).

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 the same servers as Oracle SOA Suite.

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 Real Applications Clusters (RAC) database runs on the nodes CUSTDBHOST1 and CUSTDBHOST2. The database contains the schemas needed by the Oracle SOA Suite and Oracle WebCenter Content components. The Oracle WebCenter Content and Oracle SOA Suite 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 identity management enterprise deployment.

2.1.6 About the Unicast Requirement for Communication

Oracle recommends that the nodes in the Oracle WebCenter Content enterprise deployment 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 application or custom Oracle WebCenter Content system being used.

Table 2–1  Typical Hardware Requirements

<table>
<thead>
<tr>
<th>Server</th>
<th>Disk</th>
<th>Memory</th>
<th>TMP Directory</th>
<th>Swap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>$n \times m$</td>
<td>6-8 GB</td>
<td>Default</td>
<td>Default</td>
</tr>
</tbody>
</table>

$n = \text{number of disks, at least 4 (striped as one disk)}$

$m = \text{size of the disk (minimum of 30 GB)}$

- WEBHOST
  - 10 GB
  - 4 GB
  - Default
  - Default

- SOAHOST
  - 10 GB
  - 10 GB
  - Default
  - Default

- WCCHOST
  - 10 GB
  - 10 GB
  - Default
  - Default

1 For a shared storage MW_HOME configuration, two installations suffice by making a total of 20 GB independent of the number of slots.

2 Oracle WebCenter Content can reuse MW_HOME binaries from the Oracle SOA Suite installation in shared storage.

Notes:

- 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 application or custom Oracle SOA Suite system being used.

- For WebCenter Content, Imaging, and Inbound Refinery managed servers, you need to increase the size of the heap allocated for the Java Virtual Machine (VM) on which each managed server runs to at least 1 GB (1024 MB). For more information, see "Increasing the Java VM Heap Size for Managed Servers" in the Oracle WebCenter Content Installation Guide.

### 2.3 Clock Synchronization

The clocks of all servers participating in the clusters must be synchronized to within one second difference to enable proper functioning of jobs and adapters. 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).

<table>
<thead>
<tr>
<th>Component</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database 10g or 11g</td>
<td>Oracle Database 10g (10.2.0.4 or later, Standard Edition or Enterprise Edition), using the AL32UTF8 character setOracle Database 11g (11.1.0.7 or later, Standard Edition or Enterprise Edition), using the AL32UTF8 character set<strong>Note:</strong> For Oracle WebCenter Content enterprise deployments, Oracle recommends using GridLink data sources to connect to Oracle RAC databases. To use the Oracle Single Client Access Name (SCAN) feature with GridLink, the Oracle RAC database version must be Oracle Database 11gR2 (11.2 or later, Enterprise Edition).</td>
</tr>
<tr>
<td>Repository Creation Utility (RCU)</td>
<td>Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.6)</td>
</tr>
<tr>
<td>Oracle WebLogic Server</td>
<td>Oracle WebLogic Server (10.3.6)</td>
</tr>
<tr>
<td>Oracle HTTP Server (OHS)</td>
<td>Oracle Fusion Middleware WebTier and Utilities 11g (11.1.1.6)</td>
</tr>
<tr>
<td>Oracle SOA Suite</td>
<td>Oracle SOA Suite 11g (11.1.1.6)</td>
</tr>
<tr>
<td>Oracle WebCenter Content</td>
<td>Oracle WebCenter Content 11g (11.1.1.6)</td>
</tr>
<tr>
<td>Oracle Access Manager WebGate</td>
<td>WebGate 10g (10.1.4.3) for Oracle Access Manager 10g or WebGate 11g (11.1.1.2 or later) or Oracle Access Manager 11g.</td>
</tr>
<tr>
<td>Oracle Virtual Directory</td>
<td>Oracle Identity and Access Management 11g (11.1.1.5)</td>
</tr>
<tr>
<td>Oracle Internet Directory</td>
<td>Oracle Identity and Access Management 11g (11.1.1.5)</td>
</tr>
</tbody>
</table>

2.5 Roadmap for the Reference Topology Installation and Configuration

Before beginning your Oracle WebCenter Content 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 chapter for each step.

This section covers the following topics:

- Section 2.5.1, "Flow Chart of the Oracle WebCenter Content Enterprise Deployment Process"
- Section 2.5.2, "Steps in the Oracle WebCenter Content Enterprise Deployment Process"
- Section 2.5.3, "Understanding the Incremental, Modular Approach to Enterprise Deployment"

2.5.1 Flow Chart of the Oracle WebCenter Content Enterprise Deployment Process

Figure 2–2 provides a flow chart of the Oracle WebCenter Content 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 Content Enterprise Deployment Process

Start

Review the topology diagrams and explanations

Prepare your network for enterprise deployment → Prepare your file system for enterprise deployment → Prepare your database for enterprise deployment

Install the software → Configure the web tier → Create a domain → Extend the WebLogic domain to include SOA

Extend the domain for WebCenter Content?

Yes → Extend the current domain to include Oracle WebCenter Content

No

Extend the domain for Imaging?

Yes → Extend the current domain to include Oracle WebCenter Content: Imaging

No

Extend the domain for Inbound Refinery?

Yes → Extend the current domain to include Oracle WebCenter Content: Inbound Refinery

No

Set up Node Manager

Configure server migration

Done
2.5.2 Steps in the Oracle WebCenter Content Enterprise Deployment Process

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare your network for enterprise deployment</td>
<td>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.</td>
<td>Chapter 3, “Preparing the Network for an Enterprise Deployment”</td>
</tr>
<tr>
<td>Prepare your file system for enterprise deployment</td>
<td>To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared storage.</td>
<td>Chapter 4, “Preparing the File System for an Enterprise Deployment”</td>
</tr>
<tr>
<td>Prepare your database for enterprise deployment</td>
<td>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, WCC and IMG schemas for transactional recovery privileges, and back up the database.</td>
<td>Chapter 5, “Preparing the Database for an Enterprise Deployment”</td>
</tr>
<tr>
<td>Install the software</td>
<td>Install Oracle HTTP Server, Oracle WebLogic Server, and Oracle Fusion Middleware, and apply patchsets to Oracle Fusion Middleware components.</td>
<td>Chapter 6, “Installing the Software for an Enterprise Deployment”</td>
</tr>
<tr>
<td>Configure the web tier</td>
<td>Configure the Oracle Web Tier by associating it with the WebLogic Server domain, configuring Oracle HTTP Server with the load balancer, and configuring virtual host names.</td>
<td>Chapter 7, “Configuring the Web Tier”</td>
</tr>
<tr>
<td>Create a domain</td>
<td>Run the Oracle Fusion Middleware Configuration Wizard to create a domain.</td>
<td>Chapter 8, “Creating a Domain for an Enterprise Deployment”</td>
</tr>
<tr>
<td>Extend the domain for Oracle SOA Suite</td>
<td>Extend the existing WebLogic Server domain by running the Fusion Middleware Configuration Wizard and configuring Oracle SOA Suite components.</td>
<td>Chapter 9, “Extending the Domain to Include Oracle SOA Suite Components”</td>
</tr>
<tr>
<td>Extend the domain for Oracle WebCenter Content</td>
<td>Extend the existing WebLogic domain by running the Fusion Middleware Configuration Wizard and configuring Oracle WebCenter Content.</td>
<td>Chapter 10, “Extending the Domain to Include Oracle WebCenter Content”</td>
</tr>
<tr>
<td>Extend the domain for Oracle WebCenter Content: Imaging</td>
<td>Extend the existing WebLogic domain by running the Fusion Middleware Configuration Wizard and configuring Oracle WebCenter Content: Imaging.</td>
<td>Chapter 11, “Extending the Domain to Include Imaging”</td>
</tr>
</tbody>
</table>
Table 2–3  (Cont.) Steps in the Oracle WebCenter Content Enterprise Deployment Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend the domain for Oracle WebCenter Content: Inbound Refinery</td>
<td>Extend the existing WebLogic domain by running the Fusion Middleware Configuration Wizard and configuring Oracle WebCenter Content: Inbound Refinery.</td>
<td>Section 12, &quot;Extending the Domain to Include Inbound Refinery&quot;</td>
</tr>
<tr>
<td>Set up Node Manager</td>
<td>Set up Node Manager by enabling host name verification, starting Node Manager, and configuring WebLogic Servers to use custom keystores.</td>
<td>Section 13, &quot;Setting Up Node Manager&quot;</td>
</tr>
<tr>
<td>Configure Server Migration</td>
<td>Configure server migration for the WLS_SOA1n and WLS_IMG1n managed servers. The WLS_SOA1n and WLS_IMG1n managed servers are configured to restart on SOAHOST2 and WCCHOST2, respectively, should a failure occur. The WLS_SOA2n and WLS_IMG2n managed servers are configured to restart on SOAHOST1 and WCCHOST1, respectively, should a failure occur.</td>
<td>Section 14, &quot;Configuring Server Migration for an Enterprise Deployment&quot;</td>
</tr>
<tr>
<td>Identity management integration</td>
<td>You can integrate your Oracle WebCenter Content enterprise deployment with Oracle Access Manager 10g or 11g.</td>
<td>Section 15, &quot;Integrating with Oracle Identity Management&quot;</td>
</tr>
</tbody>
</table>

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 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 Fusion Middleware Configuration Wizard again to extend the domain to include the primary Oracle Fusion Middleware product you want to use.

4. Optionally, run the Fusion Middleware 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 Fusion Middleware 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 Oracle WebCenter Content enterprise deployment 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, "Virtual Server Names Used by the Topology"
- Section 3.3, "Configuring the Load Balancer"
- Section 3.4, "IPs and Virtual IPs"
- Section 3.5, "Firewalls and Ports"
- Section 3.6, "Using 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 Virtual Server Names Used by the Topology

The Oracle WebCenter Content enterprise topology uses the following virtual server names:

- Section 3.2.1, "wcc.mycompany.com"
- Section 3.2.2, "admin.mycompany.com"
- Section 3.2.3, "soainternal.mycompany.com"
- Section 3.2.4, "wccinternal.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."

### 3.2.1 wcc.mycompany.com

`wcc.mycompany.com` is a virtual server name that acts as the access point for all HTTP traffic to the run-time Oracle WebCenter Content components. Traffic to SSL is configured. Clients access this service using the address `wcc.mycompany.com:443`.

### 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 Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control.

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.

### 3.2.3 soainternal.mycompany.com

`soainternal.mycompany.com` is a virtual server name used for internal invocations of SOA services. This URL is not exposed to the internet and is only accessible from the intranet. (For Oracle SOA Suite systems, users can set this while modeling composites or at runtime with the appropriate MBean through Fusion Middleware Control, as the URL to be used for internal services invocations.)

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

### 3.2.4 wccinternal.mycompany.com

`wccinternal.mycompany.com` is a virtual server name used for internal invocations of Oracle WebCenter Content 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 `wccinternal.mycompany.com:80` and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2.

### 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, "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."
To configure the load balancer by defining the virtual server names described in Section 3.2, "Virtual Server Names Used by the Topology," complete these steps:

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 soainternal.mycompany.com:80 and define the following rules for this virtual server:
   - For this virtual server, use your internal SOA address as the virtual server address (for example, soainternal.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.
4. Configure a virtual server in the load balancer for wcc.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, wcc.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.
5. 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.

---

**Note:** The Oracle Technology Network provides a list of validated load balancers and their configuration at http://www.oracle.com/technetwork/middleware/ias/tested-lbr-fw-sslaccel-100648.html.
- Optionally, create rules to allow access only to /console and /em on this virtual server.
- Assign the pool created in step 1 to the virtual server.

6. Configure a virtual server in the load balancer for wccinternal.mycompany.com:80 and define the following rules for this virtual server:

   - For this virtual server, use your internal Oracle WebCenter Content address as the virtual server address (for example, wccinternal.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.

7. 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 response time that you can expect from your Oracle SOA Suite 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 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 Oracle 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 the Oracle WebLogic Server migration feature. WLS_IMG1 and WLS_IMG2 also use server migration to fail over VIP4 and VIP5, respectively, from WCCHOST1 to WCCHOST2.

See the 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 WCCHOST1 and is used as the listen address by the WLS_WCC1 server. IP2 is the physical IP of WCCHOST2 and is used as the listen address by the WLS_WCC2 server.
The virtual IP db-scan.mycompany.com is the database Oracle Single Client Access Name (SCAN) address for a GridLink data source.

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

**Table 3–1 Virtual Hosts**

<table>
<thead>
<tr>
<th>Virtual IP</th>
<th>VIP Maps to...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP1</td>
<td>ADMINVHN</td>
<td>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).</td>
</tr>
<tr>
<td>VIP2</td>
<td>SOAHOST1VHN1</td>
<td>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).</td>
</tr>
<tr>
<td>VIP3</td>
<td>SOAHOST2VHN1</td>
<td>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).</td>
</tr>
<tr>
<td>VIP4</td>
<td>WCCHOST1VHN1</td>
<td>WCCHOST1VHN1 is the virtual host name that maps to the listen address for WLS_IMG1 and fails over with server migration of this managed server. It is enabled on the node where WLS_IMG1 process is running (WCCHOST1 by default).</td>
</tr>
</tbody>
</table>
Many Oracle Fusion Middleware components and services use ports. As an administrator, you must know the port numbers used by these services and ensure that the same port number is not used by two services on a host.

Most port numbers are assigned during installation. Table 3–2 lists the ports used in the Oracle WebCenter Content topology, including the ports that you must open on the firewalls in the topology.

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

### Table 3–2 Ports Used

<table>
<thead>
<tr>
<th>Type</th>
<th>Firewall</th>
<th>Port and Port Range</th>
<th>Protocol / Application</th>
<th>Inbound / Outbound</th>
<th>Other Considerations and Timeout Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser request</td>
<td>FW0</td>
<td>80</td>
<td>HTTP / Load Balancer</td>
<td>Inbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Browser request</td>
<td>FW0</td>
<td>443</td>
<td>HTTPS / Load Balancer</td>
<td>Inbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Browser request</td>
<td>FW1</td>
<td>80</td>
<td>HTTP / Load Balancer</td>
<td>Outbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Browser request</td>
<td>FW1</td>
<td>443</td>
<td>HTTPS / Load Balancer</td>
<td>Outbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Callbacks and outbound invocations</td>
<td>FW1</td>
<td>80</td>
<td>HTTP / Load Balancer</td>
<td>Outbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Type</td>
<td>Firewall</td>
<td>Port and Port Range</td>
<td>Protocol / Application</td>
<td>Inbound / Outbound</td>
<td>Other Considerations and Timeout Guidelines</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------</td>
<td>---------------------</td>
<td>--------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Callbacks and Outbound invocations</td>
<td>FW1</td>
<td>443</td>
<td>HTTPS / Load Balancer</td>
<td>Outbound</td>
<td>Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Load balancer to Oracle HTTP Server</td>
<td>n/a</td>
<td>7777</td>
<td>HTTP</td>
<td>n/a</td>
<td>See Section 3.3, &quot;Configuring the Load Balancer.&quot;</td>
</tr>
<tr>
<td>OHS registration with Administration Server</td>
<td>FW1</td>
<td>7001</td>
<td>HTTP/t3</td>
<td>Inbound</td>
<td>Set the timeout to a short period (5-10 seconds).</td>
</tr>
<tr>
<td>OHS management by Administration Server</td>
<td>FW1</td>
<td>OPMN port (6701) and OHS Admin Port (7779)</td>
<td>TCP and HTTP, respectively</td>
<td>Outbound</td>
<td>Set the timeout to a short period (5-10 seconds).</td>
</tr>
<tr>
<td>Oracle SOA Suite and Oracle WSM server access</td>
<td>FW1</td>
<td>8001 Range: 8000 - 8080</td>
<td>HTTP / WLS_SOA</td>
<td>Inbound and Outbound</td>
<td>Timeout varies based on the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Oracle WebCenter Content access</td>
<td>FW1</td>
<td>16200</td>
<td>HTTP / WLS_WCCn</td>
<td>Inbound</td>
<td>Browser-based access. Configurable session timeouts.</td>
</tr>
<tr>
<td>Oracle WebCenter Content: Imaging access</td>
<td>FW1</td>
<td>16000</td>
<td>HTTP / WLS_IMGn</td>
<td>Inbound</td>
<td>Browser-based access. Configurable session timeouts.</td>
</tr>
<tr>
<td>Imaging connection to Oracle WebCenter Content</td>
<td>n/a</td>
<td>4444</td>
<td>TCP/IP Unicast</td>
<td>n/a</td>
<td>Persistent connection. Timeout configurable on WebCenter Content Server.</td>
</tr>
<tr>
<td>Communication between SOA_Cluster members</td>
<td>n/a</td>
<td>8001</td>
<td>TCP/IP Unicast</td>
<td>n/a</td>
<td>By default, this communication uses the same port as the server’s listen address.</td>
</tr>
<tr>
<td>Communication between WCC_Cluster members</td>
<td>n/a</td>
<td>16200</td>
<td>TCP/IP Unicast</td>
<td>n/a</td>
<td>By default, this communication uses the same port as the server’s listen address.</td>
</tr>
<tr>
<td>Communication between IMG_Cluster members</td>
<td>n/a</td>
<td>16000</td>
<td>TCP/IP Unicast</td>
<td>n/a</td>
<td>By default, this communication uses the same port as the server’s listen address.</td>
</tr>
<tr>
<td>Session replication within a WebLogic Server cluster</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>By default, this communication uses the same port as the server’s listen address.</td>
</tr>
</tbody>
</table>
### Table 3–2  (Cont.) Ports Used

<table>
<thead>
<tr>
<th>Type</th>
<th>Firewall</th>
<th>Port and Port Range</th>
<th>Protocol / Application</th>
<th>Inbound / Outbound</th>
<th>Other Considerations and Timeout Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Console access</td>
<td>FW1</td>
<td>7001</td>
<td>HTTP / Administration Server and Oracle Enterprise Manager Fusion Middleware Control t3</td>
<td>Both</td>
<td>You should tune this timeout based on the type of access to the administration console (whether it is planned to use the WebLogic Server Administration Console from application tier clients or clients external to the application tier).</td>
</tr>
<tr>
<td>Node Manager</td>
<td>n/a</td>
<td>5556</td>
<td>TCP/IP</td>
<td>n/a</td>
<td>For actual values, see &quot;Firewalls and Ports&quot; in the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management.</td>
</tr>
<tr>
<td>Access Server access</td>
<td>F</td>
<td>5575 (OAM 11g)</td>
<td>OAP</td>
<td>Inbound</td>
<td>For actual values, see &quot;Firewalls and Ports&quot; in the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6021 (OAM 10g)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Server access (OAM 10g)</td>
<td>FW1</td>
<td>6022</td>
<td>OAP</td>
<td>Inbound</td>
<td></td>
</tr>
<tr>
<td>Database access</td>
<td>FW2</td>
<td>1521</td>
<td>SQL*Net</td>
<td>Both</td>
<td>Timeout depends on all database content and on the type of process model used for Oracle SOA Suite.</td>
</tr>
<tr>
<td>Coherence for deployment</td>
<td>n/a</td>
<td>8088</td>
<td></td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 8000 - 8090</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Internet Directory access</td>
<td>FW2</td>
<td>389</td>
<td>LDAP</td>
<td>Inbound</td>
<td>You should tune the directory server's parameters based on load balancer, and not the other way around.</td>
</tr>
<tr>
<td>Oracle Internet Directory access</td>
<td>FW2</td>
<td>636</td>
<td>LDAP SSL</td>
<td>Inbound</td>
<td>You should tune the directory server's parameters based on load balancer, and not the other way around.</td>
</tr>
<tr>
<td>JOC for OWSM</td>
<td>n/a</td>
<td>9991</td>
<td>TCP/IP</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 9988-9998</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser request</td>
<td>n/a</td>
<td>16250</td>
<td>HTTP / WLS_IBRr</td>
<td>n/a</td>
<td>Browser-based access. Configurable session timeouts.</td>
</tr>
</tbody>
</table>
3.6 Using 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.

An Oracle WebCenter Content enterprise deployment topology uses different domain homes for the Administration Server and the managed servers, as described in Section 4.3, "Recommended Locations for the Different Directories." Derived from this, and for integrity and consistency purposes, Oracle requires the use of an LDAP server as policy and credential store in the context of an Oracle WebCenter Content enterprise deployment topology. To configure the Oracle WebCenter Content enterprise deployment topology with an LDAP as credential and policy store, follow the steps in Section 15.2, "Credential and Policy Store Configuration."

---

**Note:** The firewall ports depend on the definition of TCP/IP ports.
Preparing the File System for an Enterprise Deployment

This chapter describes how to prepare your file system for an Oracle WebCenter Content enterprise deployment. It provides information about recommended directory structure and locations, and it 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, "Recommended Locations for the Different Directories"
- Section 4.4, "Configuring Shared Storage"
- Section 4.5, "Preparing the File System for Enterprise Deployment Summary"

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 file 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 Content 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 Oracle SOA Suite or Oracle WebCenter Content is installed.

ORACLE_COMMON_HOME: This environment variable and related directory path refers to the Oracle Common home, which contains the binary and library files required for 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.

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 Recommended Locations for the Different Directories

With Oracle Fusion Middleware 11g, you can create multiple managed servers from a 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. For maximum availability, however, Oracle recommends using redundant binary installations.

In the enterprise deployment model, two Oracle Fusion Middleware homes (MW_HOME), 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 in the following text) 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, Oracle recommends maintaining the Oracle Inventory (oraInventory) 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 in addition...
Recommended Locations for the Different Directories

Preferable Locations for the Different Directories

The following paragraphs describe the recommended directories. 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. Oracle recommends this structure in the shared storage device for consistency and simplicity.

**ORACLE_BASE:**

/u01/app/oracle

**MW_HOME (application tier):**

ORACLE_BASE/product/fmw

- Mount point: ORACLE_BASE/product/fmw
- Shared storage location: ORACLE_BASE/product/fmw (VOL1 and VOL2)
- Mounted from: Nodes alternatively mount VOL1 or VOL2 in such a way that at least half of the nodes use an installation and the other half use the other one. In the Oracle WebCenter Content enterprise deployment, SOAHOST1 and WCCHOST1 mount VOL1 and SOAHOST2 and WCCHOST2 mount VOL2. When only one volume is available, nodes mount two different directories in a shared storage alternatively (that is, 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).
Recommended Locations for the Different Directories

**ORACLE_HOME (web tier):**

**ORACLE_BASE/product/fmw/web**

- Mount point: **ORACLE_BASE/product/fmw**
- Shared storage location: **ORACLE_BASE/product/fmw (VOL1 and VOL2)**
- Mounted from: For shared storage installations, nodes alternatively mount VOL1 or VOL2 in such a way that at least half of the nodes use an installation and the other half use the other one. In the WebCenter Content enterprise deployment, WEBHOST1 would mount VOL1 and WEBHOST2 would mount VOL2. When only one volume is available, nodes mount the two suggested directories in shared storage alternatively (that is, 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).

**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.

**WL_HOME:**

**MW_HOME/wlserver_10.3**

**ORACLE_HOME:**

**MW_HOME/soa or MW_HOME/wcc**

**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).*

**ORACLE_INSTANCE (OHS instance):**

**ORACLE_BASE/admin/instance_name**

**Note:** *(VOL1) is optional; you could also use (VOL2).*
Domain Directory for Administration Server Domain Directory:

ORACLE_BASE/admin/domain_name/aserver/domain_name (The last domain_name directory is added by Fusion Middleware 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 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/Node/n/mserver/ (each node uses a different domain directory for managed servers).

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

Location of JMS file-based stores and Tlogs:

ORACLE_BASE/admin/domain_name/cluster_name/jms

ORACLE_BASE/admin/domain_name/cluster_name/tlogs

- Mount point: ORACLE_BASE/admin/domain_name/cluster_name
- Shared storage location: ORACLE_BASE/admin/domain_name/cluster_name
- Mounted from: All nodes running Oracle SOA Suite and Oracle WebCenter Content components need to mount this shared storage location so that transaction logs and JMS stores are available when server migration to another node take place.

Location of Oracle WebCenter Content: Imaging input files, images, and samples input directories:

ORACLE_BASE/admin/domain_name/img_cluster_name/input_files

ORACLE_BASE/admin/domain_name/img_cluster_name/input_files/Samples

ORACLE_BASE/admin/domain_name/img_cluster_name/images

- Mount point: ORACLE_BASE/admin/domain_name/img_cluster_name
- Shared storage location: ORACLE_BASE/admin/domain_name/img_cluster_name
- Mounted from: All nodes containing Imaging mount these locations (all nodes need to have access to input files and the images to process).

The location of input files and images may vary according to each customer’s implementation needs. It is relevant, however, that image files are located in a device isolated from other concurrent accesses that can degrade the performance of the system. A separate volume can be used for this purpose. In general, it is good practice...
to place the files under the cluster directory structure for consistent backups and maintenance.

In a multinode Imaging installation, this location is shared among all the input agents and must be accessible by all agents. If input agents are on different machines, this must be a shared network.

---

**Note:** In order to process input files, the input agent must have the appropriate permissions on the input directory and the input directory must allow file locking. The input agent requires that the user account that is running the WebLogic Server service have read and write privileges to the input directory and all files and subdirectories in the input directory. These privileges are required so that the input agent can move the files to the various directories as it works on them. File locking on the share is needed by the input agent to coordinate actions between servers in the cluster.

---

**Location of the Oracle WebCenter Content vault (native file repository):**

\[\text{ORACLE_BASE}/admin/domain_name/wcc\_cluster\_name/cs/vault\]

- **Mount point:** \[\text{ORACLE_BASE}/admin/domain_name/wcc\_cluster\_name\]
- **Shared storage location:** \[\text{ORACLE_BASE}/admin/domain_name/wcc\_cluster\_name\]
- **Mounted from:** All nodes that contain WebCenter Content mount this location (all nodes need to have access to input files and the images to process).

**Location of the Inbound Refinery directory:**

\[\text{ORACLE_BASE}/admin/domain_name/ibr\_cluster\_name\]

\[\text{ORACLE_BASE}/admin/domain_name/ibr\_cluster\_name/ibrN}\ (where \(N\) is the number of an Inbound Refinery instance)

- **Mount point:** \[\text{ORACLE_BASE}/admin/domain_name/ibr\_cluster\_name\]
- **Shared storage location:** \[\text{ORACLE_BASE}/admin/domain_name/ibr\_cluster\_name\]
- **Mounted from:** All nodes that contain Inbound Refinery mount this location.

**Location of the application directory for the Administration Server:**

\[\text{ORACLE_BASE}/admin/domain_name/aserver/applications\]

- **Mount point:** \[\text{ORACLE_BASE}/admin/domain_name/aserver/applications\]
- **Shared storage location:** \[\text{ORACLE_BASE}/admin/domain_name/aserver\]

**Location of the application directory for a managed server:**

\[\text{ORACLE_BASE}/admin/domain_name/mserver/applications\]

---

**Note:** This directory is local in the context of the Oracle WebCenter Content enterprise deployment. A shared domain directory for a managed server with Content Server does not work because certain files within the domain, such as intradoc.cfg, are specific to each node.

---

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

### Table 4–1 Directory Structure Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="admin" alt="Admin Server" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="managed" alt="Managed Server" /></td>
<td>The managed server domain directories can be on a local disk or a shared disk. Further, if you want to share the managed server domain directories on multiple nodes, then you must mount the same shared disk location across the nodes. The instance_name directory for the web tier can be on a local disk or a shared disk.</td>
</tr>
<tr>
<td><img src="fixed" alt="Fixed" /></td>
<td>Fixed name.</td>
</tr>
</tbody>
</table>
Table 4–1 (Cont.) Directory Structure Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Installation-dependent name.</td>
</tr>
</tbody>
</table>

Figure 4–2 shows an example configuration for shared storage with multiple volumes for Oracle SOA Suite.

**Figure 4–2 Example Configuration for Shared Storage**

Table 4–2 summarizes the directory structure for an Oracle WebLogic Server domain that includes Oracle SOA Suite and Oracle WebCenter Content managed servers that share storage.
<table>
<thead>
<tr>
<th>Server</th>
<th>Type of Data</th>
<th>Volume in Shared Storage</th>
<th>Directory</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLS_WCC1</td>
<td>Tx Logs</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/tlogs</td>
<td>The transaction directory is common (decided by WebLogic Server), but the files are separate.</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>Tx Logs</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/tlogs</td>
<td>The transaction directory is common (decided by WebLogic Server), but the files are separate.</td>
</tr>
<tr>
<td>WLS_WCC1</td>
<td>JMS Stores</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/jms</td>
<td>The transaction directory is common (decided by WebLogic Server), but the files are separate; for example: WCCJMSStore1, UMSJMSStore1, and so on.</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>JMS Stores</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/jms</td>
<td>The transaction directory is common (decided by WebLogic Server), but the files are separate; for example: WCCJMSStore2, UMSJMSStore2, and so on.</td>
</tr>
<tr>
<td>WLS_SOA1 and WLS_WCC1</td>
<td>WLS Install</td>
<td>VOL1</td>
<td>MW_HOME</td>
<td>Individual in each volume, but both servers see the same directory structure (SOAHOST2 and WCCHOST2 mount VOL1).</td>
</tr>
<tr>
<td>WLS_SOA1 and WLS_WCC1</td>
<td>WLS Install</td>
<td>VOL2</td>
<td>MW_HOME</td>
<td>Individual in each volume, but both servers see the same directory structure (SOAHOST2 and WCCHOST2 mount VOL2).</td>
</tr>
<tr>
<td>WLS_WCC1</td>
<td>WCC Install</td>
<td>VOL1</td>
<td>MW_HOME/wcc</td>
<td>Individual in each volume, but both servers see the same directory structure.</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>WCC Install</td>
<td>VOL2</td>
<td>MW_HOME/wcc</td>
<td>Individual in each volume, but both servers see the same directory structure.</td>
</tr>
<tr>
<td>WLS_SOA1</td>
<td>Domain Config</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/aserver/domain_name</td>
<td>Used by only one server where the Administration Server is running.</td>
</tr>
<tr>
<td>WLS_WCC1</td>
<td>Domain Config</td>
<td>VOL1</td>
<td>ORACLE_BASE/admin/domain_name/mserver/domain_name</td>
<td>Individual in each volume, but both servers see the same directory structure.</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>Domain Config</td>
<td>VOL2</td>
<td>ORACLE_BASE/admin/domain_name/mserver/domain_name</td>
<td>Individual in each volume, but both servers see the same directory structure.</td>
</tr>
<tr>
<td>WLS_WCC1</td>
<td>Web and Vault Files</td>
<td>VOL3</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/vault</td>
<td>Directory for vault files on a separate volume with locking disabled.</td>
</tr>
<tr>
<td>WLS_WCC1</td>
<td>Web and Vault Files</td>
<td>VOL3</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/weblayout</td>
<td>Directory for weblayout files on a separate volume with locking disabled.</td>
</tr>
</tbody>
</table>
4.4 Configuring Shared Storage

Use the following commands to create and mount shared storage locations so that WCCHOST1 and WCCHOST2 can see the same location for binary installation in two separate volumes.

In the commands, nasfiler is the shared storage filer.

**From SOAHOST1 and from WCCHOST1:**

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

**From SOAHOST2 and from WCCHOST2:**

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

If only one volume is available, you can provide redundancy for the binaries by using two different directories in the shared storage and mounting them to the same directory in the Oracle WebCenter Content servers:

**From SOAHOST1 and from WCCHOST1:**

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

**From SOAHOST2 and from WCCHOST2:**

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

### Note:

VOL3 is mounted as an NFS nolock volume. For details, see Section 4.4, “Configuring Shared Storage”. 

### Table 4–2 (Cont.) Contents of Shared Storage

<table>
<thead>
<tr>
<th>Server</th>
<th>Type of Data</th>
<th>Volume in Shared Storage</th>
<th>Directory</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLS_WCC2</td>
<td>Web and Vault Files</td>
<td>VOL3</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/vault</td>
<td>Directory for vault files on a separate volume with locking disabled.</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>Web and Vault Files</td>
<td>VOL3</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name/weblayout</td>
<td>Directory for weblayout files on a separate volume with locking disabled.</td>
</tr>
<tr>
<td>WLS_IBR1</td>
<td>Inbound Refinery</td>
<td>VOL3</td>
<td>ORACLE_BASE/admin/domain_name/ibr_cluster_name/ibrn</td>
<td>Directory for all Inbound Refinery files on a separate volume with locking disabled.</td>
</tr>
</tbody>
</table>

**Note:** The user ID used to create a shared storage file system owns those files and has read, write, and execute privileges for them. 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.
The following commands show how to share the Oracle WebCenter Content TX logs location across different nodes:

**From WCCHOST1:**

```
mount nasfiler:/vol/vol1/ORACLE_BASE/admin/domain_name/wcc_cluster_name/tlogs
```

**From WCCHOST2:**

```
mount nasfiler:/vol/vol1/ORACLE_BASE/admin/domain_name/wcc_cluster_name/tlogs
```

The following commands show how to share the Imaging jms location across different nodes:

**From WCCHOST1:**

```
mount nasfiler:/vol/vol1/ORACLE_BASE/admin/domain_name/img_cluster_name/jms
```

**From WCCHOST2:**

```
mount nasfiler:/vol/vol1/ORACLE_BASE/admin/domain_name/img_cluster_name/jms
```

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

**WCPAHOST1:**

```
WCPAHOST1> mount nasfiler:/vol/vol3/ORACLE_BASE/admin/wcdomain/wcc_cluster_name/vault
```

**WCPHOST1:**

```
WCPHOST1> mount nasfiler:/vol/vol3/ORACLE_BASE/admin/wcdomain/ibr_cluster_name
```

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
```
4.5 Preparing the File System for Enterprise Deployment Summary

After reading this chapter you should have an understanding of the recommended file structure defined in this guide. You should also be prepared to configure shared storage for your Oracle WebCenter Content enterprise deployment. Chapter 5, "Preparing the Database for an Enterprise Deployment" describes how to set up the database, load the metadata repository in the Oracle RAC database, and back up the database.

**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.

```
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 Content 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, "Database Requirements"
- Section 5.3, "Creating Database Services"
- Section 5.4, "Loading the Oracle Fusion Middleware Metadata Repository in the Oracle RAC Database"
- Section 5.5, "Backing Up the Database"

5.1 Overview of Preparing the Database for an Enterprise Deployment

For the Oracle WebCenter Content 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 Oracle SOA Suite and Oracle WebCenter Content components. This database is separate from the Identity Management database, which is used in the 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 distribution or from the location listed in Table 2–2. For the enterprise topology, an Oracle Real Application Clusters (RAC) database is highly recommended.

When you configure the Oracle SOA Suite components, the Fusion Middleware Configuration Wizard will prompt you to enter the information for connecting to the database that contains the metadata repository.
5.2 Database Requirements

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

- Section 5.2.1, "Database Host Requirements"
- Section 5.2.2, "Supported Database Versions"
- Section 5.2.3, "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 the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*.

- **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 Content 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:


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%";
```
5.2.3 Initialization Parameters

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

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Parameter</th>
<th>Required Value</th>
<th>Parameter Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle SOA Suite</td>
<td>PROCESSES</td>
<td>400 or greater</td>
<td>Static</td>
</tr>
<tr>
<td>Oracle WebCenter Content</td>
<td>PROCESSES</td>
<td>100 or greater</td>
<td>Static</td>
</tr>
<tr>
<td>Oracle SOA Suite and Oracle WebCenter Content</td>
<td>PROCESSES</td>
<td>500 or greater</td>
<td>Static</td>
</tr>
</tbody>
</table>

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:

```
SHOW PARAMETER processes
```

Set the initialization parameter using the following command:

```
ALTER SYSTEM SET processes=500 open_cursors=500 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

When multiple Oracle Fusion Middleware products are sharing the same database, each product should be configured to connect to a separate, dedicated database service. For more information about connecting to Oracle databases using services, see "Overview of Connecting to Oracle Database Using Services and VIP Addresses" in the Oracle Real Application Clusters Administration and Deployment Guide. For complete instructions on creating and managing database services, see "Introduction to
Automatic Workload Management” in the Oracle Real Application Clusters Administration and Deployment Guide.

Run-time connection load balancing requires configuring Oracle RAC Load Balancing Advisory with service-level goals for each service for which load balancing is enabled. You can configure the Oracle RAC Load Balancing Advisory for SERVICE_TIME or THROUGHPUT. Set the connection load-balancing goal to SHORT. For Oracle Database 10g or 11g Release 1 (11.1), use the DBMS_SERVICE package for this modification. For Oracle Database 11g Release 2 (11.2), use the Server Control Utility (SRVCTL) instead.

The Oracle WebCenter Content installation is configured to use the service wccedg.mycompany.com. For Oracle SOA Suite, using a service named soaedg.mycompany.com is recommended.

---

**Note:** For simplicity, the data source configuration screens in this guide use the same service name (wccedg.mycompany.com).

---

This section includes the following topics:

- Section 5.3.1, "Creating Database Services for 10g and 11g Release 1 (11.1) Databases"
- Section 5.3.2, "Creating Database Services for 11g Release 2 (11.2) Databases"

### 5.3.1 Creating Database Services for 10g and 11g Release 1 (11.1) Databases

You can create and modify 10g and 11g Release 1 (11.1) database services using the DBMS_SERVICE package.

**To create and modify a 10g or 11.1 database service:**

1. Log in to SQL*Plus, and create the service:

   ```sql
   sqlplus "sys/password as sysdba"
   SQL> EXECUTE DBMS_SERVICE.CREATE_SERVICE
       (SERVICE_NAME => 'wccedg.mycompany.com',
        NETWORK_NAME => 'wccedg.mycompany.com',
       );
   ```

   **Notes:**

   - For the service name of an Oracle RAC database, use lowercase letters, followed by the domain name. For example:
     `wccedg.mycompany.com`
   - Enter the EXECUTE DBMS_SERVICE command shown on a single line.
     For more information about the DBMS_SERVICE package, see the Oracle Database PL/SQL Packages and Types Reference.

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

   ```bash
   srvctl add service -d ecmbd -s wccedg.mycompany.com -r ecmbdb1,ecmbdb2
   ```
3. Start the service:

```bash
srvctl start service -d ecmdb -s wcedg.mycompany.com
```

**Note:** For complete instructions on creating and managing database services with SRVCTL, see "Administering Services with SRVCTL" in the Oracle Real Application Clusters Administration and Deployment Guide.

4. Modify the service for the appropriate service goals, with either of these EXECUTE commands:

```sql
SQL> EXECUTE DBMS_SERVICE.MODIFY_SERVICE (service_name => 'wcedg.mycompany.com', goal => DBMS_SERVICE.GOAL_THROUGHPUT, clb_goal => DBMS_SERVICE.CLB_GOAL_SHORT);
SQL> EXECUTE DBMS_SERVICE.MODIFY_SERVICE (service_name => 'wcedg.mycompany.com', goal => DBMS_SERVICE.GOAL_SERVICE_TIME, clb_goal =>DBMS_SERVICE.CLB_GOAL_SHORT);
```

5.3.2 Creating Database Services for 11g Release 2 (11.2) Databases

You can create and modify 11g Release 2 (11.2) database services using the `srvctl` command of SRVCTL.

To create and modify an 11.2 database service:

1. Log in to SQL*Plus and create the service:

```sql
sqlplus "sys/password as sysdba"

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

**Notes:**

- For the service name of an Oracle RAC database, use lowercase letters, followed by the domain name. For example:
  
  `wcedg.mycompany.com`

- Enter the `EXECUTE DBMS_SERVICE` command shown on a single line.

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

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

```bash
srvctl add service -d ecmdb -s wcedg.mycompany.com -r ecmdb1,ecmdb2
```
3. Start the service:

```
srvctl start service -d ecmdb -s wccedg.mycompany.com
```

**Note:** For complete instructions on creating and managing database services with SRVCTL, see “Administering Services with SRVCTL” in the Oracle Real Application Clusters Administration and Deployment Guide.

4. Modify the service for the appropriate service goal, with either of these `srvctl` commands:

```
srvctl modify service -d ecmdb -s wccedg.mycompany.com -B SERVICE_TIME -j SHORT
srvctl modify service -d ecmdb -s wccedg.mycompany.com -B THROUGHPUT -j SHORT
```

For more information about the different service definitions, see "Load Balancing Advisory" in the Oracle Real Application Clusters Administration and Deployment Guide.

### 5.4 Loading the Oracle Fusion Middleware 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 Content installation. This means that if you install Oracle WebCenter Content 11g Release 1 (11.1.1.6) in this enterprise deployment, you must use RCU 11g Release 1 (11.1.1.6).

To load the Oracle Fusion Middleware Repository into a database, complete these steps:

1. Open the Repository Creation Utility (RCU) distribution, and then start RCU from the bin directory in the RCU home directory:

   ```
   cd RCU_HOME/bin
   ./rcu
   ```

2. In the Welcome screen (if displayed), click Next.

3. In the Create Repository screen, select Create to load component schemas into a database. Click Next.
4. In the Database Connection Details screen (Figure 5–1), enter the connect information for your database:
   - **Database Type**: Select Oracle Database.
   - **Host Name**: Specify the name of the node on which the database resides. For the Oracle RAC database, specify the VIP name or one of the node names as the host name; for example, CUSTDBVIP1.
   - **Port**: Specify the listen port number for the database: 1521.
   - **Service Name**: Specify the service name of the database (wccedg.mycompany.com).
   - **Username**: Specify the name of the user with DBA or SYSDBA privileges: SYS.
   - **Password**: Enter the password for the SYS user.
   - **Role**: Select the database user’s role from the list: SYSDBA (required by the SYS user).

   Click Next.

**Figure 5–1 Database Connection Details Screen**

5. If your database is not using the UTF-8 character set, you will see a warning message indicating that there may be data loss if you are going to use the database for multilingual support. If you are not planning to use multilingual support, then you can click Ignore. Otherwise, click Stop.

6. In the Select Components screen (Figure 5–2), do the following:
   - **Select Create a new Prefix**, and enter a prefix to use for the database schemas, for example DEV or PROD. You can specify up to six characters as a prefix. Prefixes are used to create logical groupings of multiple repositories in a database. For more information, see the Oracle Fusion Middleware Repository Creation Utility User’s Guide.
Tip: Note the name of the schema because the upcoming steps require this information.

- Select the following components:
  - AS Common Schemas:
    - Metadata Services
  - WebCenter Content:
    - Oracle WebCenter Content Server - Complete
    - Oracle WebCenter Content: Imaging
  - SOA and BPM Infrastructure:
    - SOA Infrastructure
    - User Messaging (automatically selected with SOA Infrastructure)

Click Next.

Figure 5–2  Select Components Screen

7. In the Schema Passwords screen (Figure 5–3), 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.
8. In the Map Tablespaces screen, choose the tablespaces for the selected components, and click Next.

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

9. In the Summary screen, click Create.

10. In the Completion Summary screen, click Close.

11. Verify that the required schemas were created successfully by connecting to the database with the new user added:

   ```bash
   ORACLE_HOME/bin/sqlplus
   
   Log in as the DEV_OCS user and enter the password. A simple verification can be performed by querying the schema version registry:
   
   -bash-3.00$ $ORACLE_HOME/bin/sqlplus DEV_OCS/password as SYSDBA
   SQL> SELECT version, status FROM schema_version_registry where owner = "DEV_OCS";
   
   VERSION STATUS
   -----------------------------------------
   11.1.1.6.0 VALID
5.5 Backing Up the Database

After you have loaded the metadata repository into your database, you should 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. It is recommended that you use Oracle Recovery Manager for the database, particularly if the database was created using Oracle ASM. If possible, a cold backup using operating system tools such as tar can also be performed.

---

**Note:** Oracle recommends using the database used for identity management (see Chapter 15, "Integrating with Oracle Identity Management") to store the Oracle WSM policies. It is therefore expected that you will use the Oracle Identity Management database information for the OWSM MDS schemas, which will be different from the database information used for the rest of the Oracle SOA Suite schemas. To create the required schemas in the database, repeat the steps above using the Oracle Identity Management database information, but select only **AS Common Schemas: Metadata Services** in the Select Components screen (step 6).
This chapter describes the software installations required for the Oracle WebCenter Content enterprise deployment reference topology. You install Oracle HTTP Server and then Oracle Fusion Middleware.

Note: Before starting the setup process, read the release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at http://docs.oracle.com/cd/E23943_01/relnotes.htm.

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 Oracle Fusion Middleware (FMW) components. Later chapters describe the required configuration steps to create the Oracle WebCenter Content reference topology.

**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.

Select one of the download locations and download Oracle WebCenter Content and Oracle SOA Suite. The ZIP archive files are saved to your system.

After you download each archive file, extract it 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.
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 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:
  ```bash
  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

<table>
<thead>
<tr>
<th>Hosts</th>
<th>Oracle HTTP Server</th>
<th>Oracle WebLogic Server</th>
<th>Oracle SOA Suite</th>
<th>Oracle WebCenter Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBHOST1</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEBHOST2</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOAHOST1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SOAHOST2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WCCHOST1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WCCHOST2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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.

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 values:
   
   a. **Fusion Middleware Home Location** (installation location): `ORACLE_BASE/product/fmw`
   
   b. **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 `MW_HOME` directory after installing Oracle HTTP Server:

   a. `oracle_common`
   
   b. `web`
6.2.3 Backing Up the Installation

The Middleware home should be backed up now from WEBHOST1 (make sure no server is running at this point):

```
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 Oracle WebCenter Content enterprise deployment reference topology. 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 release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at http://docs.oracle.com/cd/E23943_01/relnotes.htm.

---

This section covers these topics:

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

### 6.3.1 Installing Oracle WebLogic Server and Creating the Middleware Home

To install Oracle WebLogic Server on SOAHOST1 and SOAHOST2:

---

**Note:** For information about running the generic installer for installing WebLogic Server on 64-bit platforms using a 64-bit JDK, see the section "Installing WebLogic Server on 64-Bit Platforms Using a 64-Bit JDK" in the Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server.

---

1. Start the installer for Oracle WebLogic Server:

```
$ ./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`.

   *ORACLE_BASE* is the base directory under which Oracle products are installed. The recommended value is `/u01/app/oracle`. See Section 4.3, "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 checkbox and click Done.

11. Validate the installation by verifying that the following directories and files appear in the MW_HOME directory after installing Oracle WebLogic Server:
   - coherence_version
   - jrockit-jdkversion
   - modules
   - registry.xml
   - utils
   - domain-registry.xml
   - logs
   - ocm.rsp
   - registry.dat
   - wlserver_10.3

### 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 Content"

#### 6.3.2.1 Installing Oracle SOA Suite

To install Oracle SOA Suite on SOAHOST1 and SOAHOST2:

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 Middleware Home."

---

**Note:** Since the installation is performed on a shared storage, the MW_HOME is accessible and used by the Oracle WebCenter Content servers in WCCHOST1 and WCCHOST2.

---

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 OS group for the user performing the installation.
   
   c. Click OK.

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

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 (Figure 6–1), 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 directory name (soa).
Click **Next** when you are done.

8. In the Application Server screen, make sure **WebLogic Server** is selected (which is the default), and click **Next**.

9. In the Installation Summary screen, click **Install**.

   The Oracle SOA Suite software is installed.

10. In the Installation Complete screen, click **Finish**.

11. Validate the installation by verifying that the following directories and files appear in the **MW_HOME** directory after installing Oracle WebLogic Server, Oracle Fusion Middleware, and Oracle SOA Suite:

    - coherence_version
    - jrockit-jdkversion
    - modules
    - oracle_common
    - registry.xml
    - utils
    - domain-registry.xml
    - logs
    - ocm.rsp
    - registry.dat
    - soa
    - wlserver_10.3
6.3.2.2 Installing Oracle WebCenter Content

When you install the Oracle WebCenter Content software suite, you install product bits for the following feature sets on your system:

- Oracle WebCenter Content
- Oracle WebCenter Content: Imaging
- Oracle WebCenter Content: Records
- Oracle WebCenter Content: Inbound Refinery

To install Oracle WebCenter Content on SOAHOST1 and SOAHOST2:

---

Note: Since the installation is performed on a shared storage, the MW_HOME is accessible and used by the Oracle WebCenter Content servers in WCCHOST1 and WCCHOST2.
---

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 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 the 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 MW_HOME directory after installing Oracle WebLogic Server, Oracle Fusion Middleware, Oracle SOA Suite, and Oracle WebCenter Content:

   - coherence_version
   - jrockit-jdkversion
   - modules
   - oracle_common
- registry.xml
- utils
- domain-registry.xml
- logs
- ocm.rsp
- registry.dat
- soa
- wlserver_10.3
- wcc

6.3.3 Backing Up the Installation

The 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 the Oracle Fusion Middleware components.
This chapter describes how to configure the Oracle web tier to support the Oracle Fusion Middleware WebCenter Content 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 Installation"
- Section 7.4, "Associating the Oracle Web Tier with the Oracle WebLogic Domain"
- Section 7.5, "Configuring Oracle HTTP Server with the Load Balancer"
- 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 Fusion Middleware 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 Oracle HTTP 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:
   
   cd ORACLE_COMMON_HOME/common/bin

2. Start the Configuration Wizard:
   
   ./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: ORACLE_BASE/admin/webn
   - AS Instance Name: webn
   - OHS Component Name: ohsn

   (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 does make 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:

   ```ini
   [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 Installation

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 via the Oracle Fusion Middleware console.

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

cd ORACLE_BASE/admin/instance_name/bin

./opmnctl registerinstance -adminHost ADMINVHN -adminPort 7001 -adminUsername weblogic

7.5 Configuring Oracle HTTP Server with the Load Balancer

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server (WEBHOST1, WEBHOST2). You do not need to enable sticky 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. Also, you should set monitors for HTTP.

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:

1. Section 7.6.1, "Editing the httpd.conf File to Define <VirtualHost> Directives"
2. Section 7.6.2, "Restarting Both Oracle HTTP Servers"
3. Section 7.6.3, "Validating the Configuration"
7.6.1 Editing the httpd.conf File to Define <VirtualHost> Directives

In order for Oracle WebCenter Content to work with the load balancer, virtual hosts need to be created in the Oracle HTTP Server configuration. Edit the httpd.conf file located in ORACLE_INSTANCE/config/OHS/ohs1 (or ohs2) and add the following entries to the <VirtualHost> section:

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

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName admin.mycompany.com:80
  RewriteEngine On
  RewriteOptions inherit
  UseCanonicalName On
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soainternal.mycompany.com:80
  RewriteEngine On
  RewriteOptions inherit
  UseCanonicalName On
</VirtualHost>
```

7.6.2 Restarting Both Oracle HTTP Servers

Restart both Oracle HTTP Servers after modifying the httpd.conf files. On both WEBHOST1 and WEBHOST2, execute the following commands:

```
cd ORACLE_BASE/admin/instance_name/bin

opmnctl stopall

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:

- http://WEBHOST1.mycompany.com:7777/
- http://WEBHOST2.mycompany.com:7777/

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 Oracle Fusion Middleware Configuration Wizard, Oracle WebLogic Server Administration Console, and Oracle Enterprise Manager Fusion Middleware Control. You can extend the domain to add Fusion Middleware (FMW) components: Oracle SOA Suite, Oracle WebCenter Content and, optionally, Oracle WebCenter Content: Imaging and Oracle WebCenter Content: Inbound Refinery. This will be addressed in later chapters in this document.

**Note:** Before starting the setup process, read the release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at [http://docs.oracle.com/cd/E23943_01/relnotes.htm](http://docs.oracle.com/cd/E23943_01/relnotes.htm).

This chapter contains the following sections:

- Section 8.1, "Overview of Creating a Domain"
- Section 8.2, "Enabling ADMINVHN on 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, "Configuring Oracle HTTP Server for the WebLogic Domain"
- Section 8.6, "Backing Up the WebLogic Server Domain Configuration"

### 8.1 Overview of Creating a Domain

Table 8–1 lists the steps for creating a WebLogic domain, including post-configuration tasks.
Enabling ADMINVHN on SOAHOST1

After this domain is created and configure, you can extend the domain to include Oracle SOA Suite and Oracle WebCenter Content components, as described in the next chapters.

8.2 Enabling ADMINVHN on SOAHOST1

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

You are associating the Administration Server with a virtual host name (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 Oracle WebCenter Content 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 IP_address netmask netmask
   /sbin/arping -q -U -c 3 -I interface IP_address
   ```
   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, and so on`).

---

### Table 8–1 Steps for Creating a WebLogic Domain

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling VIP1 in SOAHOST1</td>
<td>Enable ADMINVHN for the SOAHOST1 hostname.</td>
<td>Section 8.2, &quot;Enabling ADMINVHN on SOAHOST1&quot;</td>
</tr>
<tr>
<td>Create a WebLogic Domain</td>
<td>Run the Configuration Wizard to create a WebLogic domain.</td>
<td>Section 8.3, &quot;Running the Configuration Wizard on SOAHOST1 to Create a Domain&quot;</td>
</tr>
<tr>
<td>Post-Configuration and Verification Tasks</td>
<td>Follow the instructions for post-configuration and validation tasks.</td>
<td>Section 8.4, &quot;Post-Configuration and Verification Tasks&quot;</td>
</tr>
<tr>
<td>Configure the Oracle HTTP Server with the WebLogic domain</td>
<td>Configure Oracle HTTP Server with the WebLogic domain and validate the configuration.</td>
<td>Section 8.5, &quot;Configuring Oracle HTTP Server for the WebLogic Domain&quot;</td>
</tr>
<tr>
<td>Back Up the Domain</td>
<td>Back up the newly configured WebLogic domain.</td>
<td>Section 8.6, &quot;Backing Up the WebLogic Server Domain Configuration&quot;</td>
</tr>
</tbody>
</table>
8.3 Running the Configuration Wizard on SOAHOST1 to Create a Domain

Run the Oracle Fusion Middleware Configuration Wizard from the Oracle Common home directory to create a domain containing the Administration Server. You will extend the domain to contain other components later.

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, it is recommended that all instances are running, so that the validation checks later on becomes more reliable.

2. On SOAHOST1, change the directory to the location of the Oracle Fusion Middleware Configuration Wizard (created in Chapter 6, "Installing the Software for an Enterprise Deployment"):

   cd ORACLE_COMMON_HOME/common/bin

3. Start the Configuration Wizard:

   ./config.sh

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

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

---

**Figure 8–1 Select Domain Source Screen**

![Select Domain Source Screen](image)

---
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]**

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

- **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**
- **Oracle JRF - 11.1.1.0 [oracle_common]**

Click **Next**.

6. In the Specify Domain Name and Location screen, enter the domain name `domain_name`.

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": enter `ORACLE_BASE/admin/domain_name/aserver` for the domain directory and `ORACLE_BASE/admin/domain_name/aserver/applications` for the application directory. This directory should be in shared storage.

Click **Next**.

7. In the Configure Administrator User Name and Password screen, enter the user name and password to be used for the domain's administrator.

Click **Next**.

8. 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**.

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

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

Click **Next**.

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

- **Name**: AdminServer
- **Listen address**: ADMINVHN.
- **Listen port**: 7001
- **SSL listen port**: N/A
- **SSL enabled**: Leave this checkbox unselected.

Click **Next**.

11. In the Configure Managed Servers screen, click **Next**.
12. In the Configure Clusters screen, click Next.

13. In the Configure Machines screen, open the Unix Machine tab and then click Add to add the following machine:

<table>
<thead>
<tr>
<th>Name</th>
<th>Node Manager Listen Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMINVHN</td>
<td>localhost</td>
</tr>
</tbody>
</table>

Leave all other fields set to their default values. Please note that the machine name does not need to be a valid host name or listen address; it is just a unique identifier of a Node Manager location.

Click Next.

14. In the Assign Servers to Machines screen, assign The Administration Server to a machine as follows:

- ADMINVHN:
  - AdminServer

Click Next.

15. In the Configuration Summary screen, click Create.

16. 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, "Verifying the RAC Database Service"
- Section 8.4.2, "Creating boot.properties for the Administration Server on SOAHOST1"
- Section 8.4.3, "Starting Node Manager on SOAHOST1"
- Section 8.4.4, "Starting the Administration Server on SOAHOST1"
- Section 8.4.5, "Validating the Administration Server Configuration"
- Section 8.4.6, "Disabling Host Name Verification for the Administration Server"

8.4.1 Verifying the RAC Database Service

Start both RAC database instances and verify that the service is up and running.

8.4.2 Creating boot.properties for the Administration Server on SOAHOST1

Create a boot.properties file for the Administration Server on SOAHOST1. This file enables the Administration Server to start without prompting you for the administrator user name and password.

1. Create the following directory structure on SOAHOST1:

```
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 directory created in the previous step, and enter the following lines in the file:

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

**Note:** When you start the Administration Server, the user name and password entries in the file get encrypted. You start the Administration Server in Section 8.4.4, “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.

### 8.4.3 Starting Node Manager on SOAHOST1

To start Node Manager on SOAHOST1, set the `StartScriptEnabled` property to `true`, and then start Node Manager using `startNodeManager.sh`.

To start Node Manager on SOAHOST1:

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:

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

   **Note:** You must use the `StartScriptEnabled` property to avoid class loading failures and other problems. See also Section 16.11.3, "Incomplete Policy Migration After Failed Restart of SOA Server."

2. Start Node Manager:

   ```bash
cd $WL_HOME/server/bin
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
./startNodeManager.sh
```

   **Note:** It is important that the `-DDomainRegistrationEnabled=true` parameter is set whenever a Node Manager is started which must manage the Administration Server. If there is no Administration Server on the machine and the machine is not an Administration Server failover node, then Node Manager can be started using `./startNodeManager.sh` (without the `export` command).
8.4.4 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 default user name and password that the Oracle Fusion Middleware Configuration Wizard set for Node Manager. You must therefore use the start script for the Administration Server for the first start. Follow these steps to start the Administration Server using Node Manager (steps 1 through 4 are required for the first start; all subsequent starts require only step 4):

1. On SOAHOST1, start the Administration Server using the start script in the domain directory:
   
   ```
   cd ORACLE_BASE/admin/domain_name/aserver/domain_name/bin
   ./startWebLogic.sh
   ```

2. Use the Administration Console to update the Node Manager credentials:
   
   
   b. Log in as the administrator.
   
   c. Click Lock & Edit.
   
   d. Click `domain_name`, then Security, then General, and then expand the Advanced options at the bottom.
   
   e. Enter a new user name 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, either by using Ctrl+C in the shell where it was started or by the standard process identification and kill commands in the operating system.

4. Start the Oracle WebLogic Scripting Tool (WLST), 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
   ```

Note: Verify that Node Manager is using the appropriate stores and alias from the Node Manager output. Node Manager should prompt out the following:

```
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/appIdentityKeyStore.jks
CustomIdentityAlias=appIdentityX
```

Host name verification works if you apply a test configuration change to the servers, and it succeeds without Node Manager reporting any SSL errors.
Once in the WLST shell, execute the following command (make sure Node Manager is up and running):

```
wlst:/offline>nmConnect("Admin_User","Admin_Pasword", "SOAHOST1","5556", "domain_name","/u01/app/oracle/admin/domain_name/aserver/domain_name")
wls:/nm/domain_name> nmStart("AdminServer")
```

**Note:** SOAHOST1 is the address of the node where the domain was created, not the listen address of the Administration Server. Also, the user name and password are only used to authenticate connections between Node Manager and clients. They are independent from the server admin ID and password, and are stored in the ORACLE_BASE/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties file.

### 8.4.5 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 in to the WebLogic Server Administration Console and verifying the cluster is listed, and then log in to Oracle Enterprise Manager Fusion Middleware Control.

To verify that the Administration Server is properly configured:

1. Open a Web browser and go to http://ADMINVHN:7001/console.
2. Log in as the administrator.
3. Check that you can access Fusion Middleware Control at http://ADMINVHN:7001/em.
4. Log in to Fusion Middleware Control with the user name and password you specified in Section 8.4.2, "Creating boot.properties for the Administration Server on SOAHOST1."

The Administration Server should be up and running.

### 8.4.6 Disabling Host Name Verification for the Administration Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 13, "Setting Up Node Manager"). If you have not configured the server certificates, you will receive errors when managing the different WebLogic servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete, as described in Chapter 13, "Setting Up Node Manager."

To disable host name verification:

1. Log in to WebLogic Server Administration Console.
2. Click Lock & Edit.
3. Expand the Environment node in the Domain Structure window.
4. Click Servers.
5. On the Summary of Servers page, select AdminServer(admin) in the Names column of the table.
6. On the settings page for the server, open the SSL tab.
7. Expand the Advanced section of the page.
8. Set host name verification to None.
9. Click Save.
10. Save and activate the changes.
11. The change will not take effect until the Administration Server is restarted (Node Manager must be up and running):
   a. Stop the Administration Server using the following command:
      
      ```
      wls:/nm/domain_name>nmKill("AdminServer")
      ```
   b. Start the Administration Server again as described in Section 8.4.4, “Starting the Administration Server on SOAHOST1.”

8.5 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 8.5.1, "Configuring Oracle HTTP Server for the Administration Server"
- Section 8.5.2, "Turning on the WebLogic Plug-In enabled Flag"
- Section 8.5.3, "Registering Oracle HTTP Server with WebLogic Server"
- Section 8.5.4, "Setting the Frontend URL for the Administration Console and Setting Redirection Preferences"
- Section 8.5.5, "Validating Access Through Oracle HTTP Server"
- Section 8.5.6, "Verifying Manual Failover of the Administration Server"

8.5.1 Configuring Oracle HTTP Server for the Administration Server

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

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the file `ORACLE_INSTANCE/config/OHS/component_name/mod_wl_ohs.conf`:

   ```
   # Admin Server and EM
   <Location /console>
   SetHandler weblogic-handler
   WebLogicHost ADMINVHN
   WeblogicPort 7001
   WLProxySSL OFF
   WLProxySSLPassThrough OFF
   </Location>
   ```

   ```
   # Admin Server and EM
   <Location /consolehelp>
   SetHandler weblogic-handler
   WebLogicHost ADMINVHN
   WeblogicPort 7001
   WLProxySSL OFF
   WLProxySSLPassThrough OFF
   </Location>
   ```
<Location /em>
  SetHandler weblogic-handler
  WebLogicHost ADMINVHN
  WeblogicPort 7001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

2. For each of the web servers on WEBHOST1 and WEBHOST2, make sure the file ORACLE_INSTANCE/config/OHS/component_name/httpd.conf includes the following lines:

   NameVirtualHost *:7777
   <VirtualHost *:7777>
     ServerName admin.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.

3. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

   ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohsX

   For WEBHOST1, use ohs1 for ias-component and for WEBHOST2 use ohs2.

### 8.5.2 Turning on the WebLogic Plug-In enabled Flag

For security purposes, and since the load balancer terminates SSL requests (Oracle HTTP Server routes the requests as non-SSL to WebLogic Server), once SSL is configured for the load balancer, turn on the WebLogic plug-in enabled flag for the domain. Make sure you do this only if SSL is configured for the load balancer. To perform this procedure, follow these steps:

1. Log in to the Administration Console.
2. Click the domain name in the navigation tree on the left.
3. Open the Web Applications tab.
4. Click Lock & Edit.
5. Select the WebLogic Plugin Enabled checkbox.
6. Save and activate the changes.
7. Restart the Administration Server (even if the Administration Console does not specifically prompt for that).

### 8.5.3 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 on WEBHOST1:

```
cd ORACLE_BASE/admin/instance_name/bin
./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 Fusion Middleware Control. To verify this, log in to Fusion Middleware Control. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

### 8.5.4 Setting the Frontend URL for the Administration Console and Setting Redirection Preferences

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

The 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 WebLogic Server Administration Console.
2. Click *Lock & Edit*.
3. Expand the *Environment* node in the Domain Structure window.
4. Click *Servers*.
5. On the Summary of Servers page, select *Admin Server* in the Names column of the table.
6. On the settings page for AdminServer(admin), open the *Protocols* tab.
7. Open the *HTTP* tab.
8. Set the *Front End Host* field to `admin.mycompany.com` and the *Frontend HTTP Port* field 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 WebLogic Server Administration Console so that the console does not trigger the reloading of configuration pages when activation of changes occurs.
   a. Log in to the WebLogic Server Administration Console.
   b. Click the *Preferences* link in the banner.
   c. Open the *Shared Preferences* tab.
   d. Clear the *Follow Configuration Changes* checkbox.
   e. Click *Save*. 
8.5.5 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as Running in the Administration Console. If the server is shown as Starting or Resuming, wait for the server status to change to Started. If another status is reported (such as Admin or Failed), check the server output log files for errors. See Section 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

Validate access to the Administration Console and Oracle Enterprise Manager Fusion Middleware Control through both Oracle HTTP Server instances, using the following URLs:

- http://WEBHOST1:7777/console
- http://WEBHOST2:7777/console
- http://WEBHOST1:7777/em
- http://WEBHOST2:7777/em
- http://admin.mycompany.com/console
- http://admin.mycompany.com/em

After you set 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 registering Oracle HTTP Server as described in Section 8.5.3, "Registering Oracle HTTP Server with WebLogic Server," it should appear as a manageable target in Fusion Middleware Control. To verify this, log in to Fusion Middleware Control. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

8.5.6 Verifying Manual Failover of the Administration Server

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:

- Section 8.5.6.1, "Assumptions and Procedure"
- Section 8.5.6.2, "Validating Access to SOAHOST2 Through Oracle HTTP Server"
- Section 8.5.6.3, "Failing the Administration Server Back to SOAHOST1"
8.5.6.1 Assumptions and Procedure

Please note the following assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on ANY address. See step 13 in Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain".
- The Administration Server is failed over from SOAHOST1 to SOAHOST2, and the two nodes have these IP addresses:
  - 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 Chapter 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).

Procedure

The following procedure shows how to fail over the Administration Server to a different node (SOAHOST2):

1. Stop the Administration Server if it is running.
2. Migrate the IP address 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 eth0:1 100.200.140.206 netmask 255.255.255.0
   ```
   c. Update the routing tables on SOAHOST2 using arping, for example:

   ```
   /sbin/arping -b -A -c 3 -I eth0 100.200.140.206
   ```
3. Start Node Manager in SOAHOST2 as described in Section 8.4.3, "Starting Node Manager on SOAHOST1."

Note: Make sure that the netmask and interface to be used match the available network configuration in SOAHOST2. Also, make sure that the location of the Administration Server application directory is mounted as described in Section 4.3, "Recommended Locations for the Different Directories."
4. Start the Administration Server on SOAHOST2 as described in Section 8.4.4, "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 WebLogic Server Administration Console at http://ADMINVHN:7001/console.
   b. Check that you can access and verify the status of components in Oracle Enterprise Manager Fusion Middleware Control at http://ADMINVHN:7001/em.

8.5.6.2 Validating Access to SOAHOST2 Through Oracle HTTP Server
Perform the same steps as in Section 8.5.5, "Validating Access Through Oracle HTTP Server." This is to check that you can access the Administration Server when it is running on SOAHOST2.

8.5.6.3 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 again. To do this, migrate ADMINVHN back to the SOAHOST1 node as follows:

1. Make sure the Administration Server is not running.
2. Run the following command on SOAHOST2:
   ```bash
   /sbin/ifconfig ethZ:N down
   ```
3. Run the following command on SOAHOST1:
   ```bash
   /sbin/ifconfig ethX:Y 100.200.140.206 netmask 255.255.255.0
   ```

   **Note:** Make sure that the netmask and interface to be used match the available network configuration in SOAHOST1.

4. Update the routing tables using arping. Run the following command from SOAHOST1:
   ```bash
   /sbin/arping -b -A -c 3 -I ethZ 100.200.140.206
   ```

5. Start the Administration Server again on SOAHOST1 as described in Section 8.4.4, "Starting the Administration Server on SOAHOST1."

6. Test that you can access the WebLogic Server Administration Console at http://ADMINVHN:7001/console.

7. Check that you can access and verify the status of components in Oracle Enterprise Manager Fusion Middleware Control at http://ADMINVHN:7001/em.

8.6 Backing Up the WebLogic Server Domain Configuration
After you have verified that the extended domain is working, perform a backup to save your domain configuration. 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 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 for information on database backup.

To back up the installation from at this point:

1. Back up the web tier from WEBHOST1:
   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 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. Repeat step 1 for WEBHOST2.

3. 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.

4. Stop the Administration Server and back up its domain directory to save your domain configuration. The configuration files all exist in the `ORACLE_BASE/admin/domain_name` directory. Run the following command on SOAHOST1 to create the backup:

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

Do not forget to restart the Administration Server again.
Backing Up the WebLogic Server Domain Configuration
Extending the Domain to Include Oracle SOA Suite Components

This chapter describes how to use the Oracle Fusion Middleware Configuration Wizard to extend the domain created in Chapter 8, "Creating a Domain for an Enterprise Deployment," to include Oracle SOA Suite components and Oracle WSM Policy Manager. You can extend the resulting domain to add other Fusion Middleware components, as described in the next chapters. It is assumed that a SOA Oracle home (binaries) has already been installed and is available from SOAHOST1 and SOAHOST2 and that a domain with an Administration Server has been created. This is the domain that will be extended in this chapter to support Oracle SOA Suite components.

Note: Before starting the setup process, read the release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at http://docs.oracle.com/cd/E23943_01/relnotes.htm.

This chapter contains the following sections:

- Section 9.1, "Overview of Extending the Domain for Oracle SOA Suite Components"
- Section 9.2, "Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2"
- Section 9.3, "Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard"
- Section 9.4, "Configuring Oracle Coherence for Deploying Composites"
- Section 9.5, "Completing Post-Configuration and Verification Tasks"
- Section 9.6, "Configuring the Java Object Cache for Oracle Web Services Manager"
- Section 9.7, "Configuring Oracle HTTP Server for the WLS_SOA Managed Servers"
- Section 9.8, "Setting the Frontend HTTP Host and Port"
- Section 9.9, "Validating Access Through Oracle HTTP Server"
- Section 9.10, "Configuring a Default Persistence Store for Transaction Recovery"
- Section 9.11, "Enabling High Availability for Oracle File and FTP Adapters"
- Section 9.12, "Scaling the Oracle Database Adapter"
- Section 9.13, "Configuring Node Manager for the WLS_SOA Managed Servers"
9.1 Overview of Extending the Domain for Oracle SOA Suite Components

Extend the WebLogic domain to include Oracle SOA Suite components. Table 9–1 lists the steps for configuring Oracle SOA Suite and other tasks required for extending the domain for Oracle SOA Suite components.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for extending the domain for Oracle SOA Suite components</td>
<td>Enable a VIP mapping for each of the host names, and synchronize the system clocks for the SOA WebLogic Server cluster</td>
<td>Section 9.2, &quot;Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2&quot;</td>
</tr>
<tr>
<td>Extend the domain for Oracle SOA Suite components</td>
<td>Extend the WebLogic domain you created in Chapter 8, “Creating a Domain for an Enterprise Deployment.”</td>
<td>Section 9.3, &quot;Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard&quot;</td>
</tr>
<tr>
<td>Configure Oracle Coherence for deploying composites</td>
<td>Configure Oracle Coherence to use unicast communication for deploying composites.</td>
<td>Section 9.4, &quot;Configuring Oracle Coherence for Deploying Composites&quot;</td>
</tr>
<tr>
<td>Complete post-configuration and verification tasks</td>
<td>Follow these instructions for post-configuration and validation tasks.</td>
<td>Section 9.5, &quot;Completing Post-Configuration and Verification Tasks&quot;</td>
</tr>
<tr>
<td>Verify the configuration of GridLink data sources and Oracle Notification Service (ONS)</td>
<td>Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.</td>
<td>Section 9.5.3, &quot;Validating GridLink Data Sources&quot;</td>
</tr>
<tr>
<td>Propagate the Domain Configuration to SOAHOST2</td>
<td>Propagate the start scripts and classpath configuration from the Administration Server’s domain directory to the managed server domain directory.</td>
<td>Section 9.5.6, &quot;Propagating the Domain Configuration to SOAHOST2&quot;</td>
</tr>
<tr>
<td>Configure Oracle HTTP Server with the extended domain</td>
<td>Configure the Oracle HTTP Server with the managed servers, validate access, set the frontend HTTP host and port, and set the WebLogic Server cluster address for SOA_Cluster.</td>
<td>Section 9.7, &quot;Configuring Oracle HTTP Server for the WLS_SOA Managed Servers&quot;</td>
</tr>
<tr>
<td>Configure a default persistence store</td>
<td>Configure a default persistence store for transaction recovery.</td>
<td>Section 9.10, &quot;Configuring a Default Persistence Store for Transaction Recovery&quot;</td>
</tr>
<tr>
<td>Configure Oracle adapters</td>
<td>Enable high availability for Oracle JCA Adapter for Files and Oracle JCA Adapter for FTP, enable high availability for the Oracle JCA Adapter for JMS, and scale the Oracle JCA Adapter for Database.</td>
<td>Section 9.12, &quot;Scaling the Oracle Database Adapter&quot;</td>
</tr>
<tr>
<td>Back up the Oracle SOA Suite configuration</td>
<td>Back up the newly extended domain configuration.</td>
<td>Section 9.15, &quot;Backing Up the Installation&quot;</td>
</tr>
</tbody>
</table>
9.2 Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2

This step is required for server migration of WLS_SOA1 and WLS_SOA2. You will associate the WLS_SOA1 and WLS_SOA2 servers with virtual host names (SOAHOST1VHN1 and SOAHOST2VHN1). Check that these virtual host names are enabled by DNS or /etc/hosts resolution in your system and that they map to the appropriate VIPs (VIP2 and VIP3).

To enable the virtual IP, run the `ifconfig` command as root:

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

For example:

```
/sbin/ifconfig ethX:Y 100.200.140.205 netmask 255.255.255.0
```

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

```
/sbin/arping -q -U -c 3 -I ethX 100.200.140.205
```

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

```
/bin/ping 100.200.140.205
```

---

**Note:** In these examples, `ethX` is the ethernet interface (eth0 or eth1) and `Y` is the index (0, 1, 2, and so on).

---

9.3 Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard

Use the Oracle Fusion Middleware Configuration Wizard to extend the domain created in Chapter 8, "Creating a Domain for an Enterprise Deployment" to support Oracle Web Services Manager and Oracle SOA Suite components.

---

**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 Oracle SOA Suite 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. On SOAHOST1, change the directory to the location of the Oracle Fusion Middleware Configuration Wizard. This is within the Oracle Common home directory (domain extensions are run from the node 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, which Figure 9–1 shows, do the following:
   a. Select **Extend my domain automatically to support the following added products**.
   
   b. Select these products:
      - Oracle SOA Suite - 11.1.1.0 [soa]
      - Oracle WSM Policy Manager - 11.1.1.0 [oracle_common] (automatically selected with Oracle SOA Suite)
      - The following products should already be selected and grayed out. They were selected when you created the domain (Section 8.3).
        - Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3]
        - Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
        - Oracle JRF - 11.1.1.0 [oracle_common]

   c. Click **Next**.

Figure 9–1 Select Extension Source Screen for Oracle SOA Suite
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, which Figure 9–2 shows, do the following:
   b. For the RAC configuration, you can select Convert to GridLink or Convert to RAC multi data source (described in Appendix A, "Using Multi Data Sources with Oracle RAC"). For the instructions given here, select Convert to GridLink.

   After you select a RAC configuration, all selected schemas are grayed.

   **Figure 9–2  Configure JDBC Component Schema Screen for Oracle SOA Suite**

   ![Configure JDBC Component Schema Screen for Oracle SOA Suite](image)

   c. Click Next.

10. In the Configure GridLink RAC Component Schema screen, which Figure 9–3 shows, do the following:
   a. Select only the SOA Infrastructure row.
b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

- **Driver**: Select Oracle driver (Thin) for GridLink Connections, Versions: 10 and later.

- **Service Name**: Enter the service name of the Oracle RAC database in lowercase letters, followed by the domain name; for example, `wccedg.mycompany.com`.

- **Username**: Enter the complete user name for the database schema owner of the corresponding component.

  This book uses **DEV** as the prefix of user names for the database schemas.

- **Password**: Enter the password for the database schema owner.

- Select **Enable FAN**.

- **Enable SSL**: Leave this option deselected.

  If you select SSL to enable Oracle Notification Service (ONS) notification encryption, provide the appropriate **Wallet File** and **Wallet Password** details.

- **Service listener**: Enter the Oracle Single Client Access Name (SCAN) address and port for the Oracle RAC database being used. The protocol should be **TCP**.
Oracle recommends that you use a SCAN address to specify the Service Listener (and OSN Host) so you do not need to update a GridLink data source containing a SCAN address if you add or remove Oracle RAC nodes. To determine the SCAN address, query the `remote_listener` parameter in the database:

```sql
SQL> show parameter remote_listener;
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_listener</td>
<td>string</td>
<td>db-scan.mycompany.com:1521</td>
</tr>
</tbody>
</table>

**Note:** For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener; for example:

- `custdbhost1-vip.mycompany.com (port 1521)`
- `custdbhost2-vip.mycompany.com (1521)`

For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database. For information about configuring multi data sources, see Appendix A, "Using Multi Data Sources with Oracle RAC."

---

- **ONS Host:** Enter here also the SCAN address for the RAC database and the ONS remote port, as reported by the database:

  ```bash
  [orc1@CUSTDBHOST2 ~]$ srvctl config nodeapps -s
  ONS exists: Local port 6100, remote port 6200, EM port 2016
  ```

**Note:** For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service; for example:

- `custdbhost1.mycompany.com (port 6200)`
- `custdbhost2.mycompany.com (6200)`

---

c. Select each data source, one at a time, and enter appropriate values for the user names and passwords.

d. Ensure that all values are correct for all schemas (SOA Infrastructure, User Messaging Service, OWSM MDS Schema, and SOA MDS Schema), and then click **Next**.
Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard

**Note:** Oracle recommends using the database used for identity management (see Chapter 15, "Integrating with Oracle Identity Management") to store the Oracle WSM policies. It is therefore expected that you will use the Oracle Identity Management database information that has been seeded through RCU (as recommended in Chapter 3, "Preparing the Network for an Enterprise Deployment") to store the WSM metadata and that this Oracle Identity Management database information will be used in this screen for the OWSM MDS schemas. (This database connection information will be different from the one used for the rest of the Oracle SOA Suite schemas.)

11. In the Test JDBC Component Schema screen, (Figure 9-4), select each schema, and then click **Test Connections**.

   The **Connection Results Log** displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen, correct your entries, and then retry the test.

   **Figure 9-4 Test JDBC Component Schema Screen**

   ![Test JDBC Component Schema Screen](image)

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

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

   - JMS Distributed Destination
   - Managed Servers, Clusters and Machines
   - Deployment and Services
   - JMS File Store

   Click **Next**.
13. In the Select JMS Distributed Destination Type screen, do the following:
   - Select UDD from the drop-down list for UMSJMSSystemResource.
   - Select UDD from the drop-down list for SOAJMSModule.
   If an override warning appears, click OK to acknowledge it.

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 add a new server called WLS_SOA2. Give these servers the attributes listed in Table 9–2. Do not modify the other servers that are shown in this screen; leave them as they are.

```
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         |
```

   Click Next.

15. In the Configure Clusters screen, add the clusters as listed in Table 9–3.

```
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 |
```

   Click Next.

**Note:** For async request/response interactions over direct binding, the SOA composites must provide their JNDI provider URL for the invoked service to look up the beans for callback.

If soa-infra config properties are not specified, but the WebLogic Server Cluster address is specified, the cluster address from the JNDI provider URL is used. This cluster address can be either a single DNS name that maps to the IP addresses of the clustered servers or a comma-separated list of server ip:port. Alternatively, the soa-infra config property JndiProviderURL/SecureJndiProviderURL can be used for the same purpose if explicitly set by users.

16. In the Assign Servers to Clusters screen, assign servers to clusters as follows:
   - **SOA_Cluster**:
     - WLS_SOA1
     - WLS_SOA2
   Click Next.
17. In the Configure Machines screen, delete the LocalMachine that appears by default and open the Unix Machine tab. You should add the SOAHOST1 and SOAHOST2 machines and eventually have the following entries:

<table>
<thead>
<tr>
<th>Name</th>
<th>Node Manager Listen Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAHOST1</td>
<td>SOAHOST1</td>
</tr>
<tr>
<td>SOAHOST2</td>
<td>SOAHOST2</td>
</tr>
<tr>
<td>ADMINVHN</td>
<td>localhost</td>
</tr>
</tbody>
</table>

Do not modify the other assignments that are shown in this screen; leave them as they are. Please note that the machine names do not need to be valid host names or listen addresses; they are just unique identifiers of Node Manager locations.

Click Next.

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

- **ADMINVHN**:
  - AdminServer
- **SOAHOST1**:
  - WLS_SOA1
- **SOAHOST2**:
  - WLS_SOA2

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.)
- **WSM-PM** should be targeted only to **SOA_Cluster**.
- The **oracle.rules#*, oracle.sdp.*, and oracle.soa.*** deployments should be targeted only to **SOA_Cluster**.

Click Next.

20. In the Target Services to Clusters or Servers screen, 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, “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.

The domain is extended to include the Oracle SOA Suite components.

23. In the Extending Domain screen, click Done.

24. Restart the Administration Server for these changes to take effect.
9.4 Configuring Oracle Coherence for Deploying Composites

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

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

---

**Note:** An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the Oracle SOA Suite system from starting. The deployment framework must be properly customized for the network environment on which the Oracle SOA Suite 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` system property, where `n` is a number between 1 and 9. You can specify up to 9 nodes as Well Known Addresses, but can have more than 9 nodes in the cluster. 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 Oracle SOA Suite server as the listener addresses (SOAHOST1VHN1 and SOAHOST2VHN1). Set this property by adding the `-Dtangosol.coherence.localhost` parameter to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab (Figure 9–5).

**Tip:** To guarantee high availability during deployments of Oracle SOA Suite 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 is listening (in SOAHOST1). SOAHOST2VHN1 is the virtual host name that maps to the virtual IP where WLS_SOA2 is listening (in SOAHOST2).
9.4.2 Specifying the Host Name

To specify the host name used by Oracle Coherence:

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure window, expand the Environment node.
3. Click Servers.
4. On the Summary of Servers page, click the name of the server (WLS_SOA1 or WLS_SOA2), which are represented as hyperlinks in the Name column of the table.
5. On the settings page for the selected server, click Lock & Edit.
6. Open the Configuration tab and then the Server Start tab.
7. Enter the following for WLS_SOA1 and WLS_SOA2 in the Arguments field.

For WLS_SOA1, enter the following (on a single line, without a carriage return):

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

For WLS_SOA2, enter the following (on a single line, without a carriage return):

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

**Note:** All arguments above are entered in one single line; that is, do not insert new lines in the Java arguments field in the Administration Console. Also, do not copy and paste the preceding text to your Administration Console's arguments text field. This may result in extraneous characters being inserted in the Java arguments. The text should not contain text or characters other than the ones shown in the preceding entry.
The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) using the `-Dtangosol.coherence.wkan.port` and `-Dtangosol.coherence.localport` startup parameters, for example:

- **WLS_SOIA1** (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.wka1.port=8089`
  - `-Dtangosol.coherence.wka2.port=8089`
  - `-Dtangosol.coherence.localport=8089`

- **WLS_SOIA2** (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.wka1.port=8089`
  - `-Dtangosol.coherence.wka2.port=8089`
  - `-Dtangosol.coherence.localport=8089`

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. Oracle SOA Suite 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.
Completing 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 Servers"
- Section 9.5.2, "Restarting Node Manager on SOAHOST1"
- Section 9.5.3, "Validating GridLink Data Sources"
- Section 9.5.4, "Propagating the Domain Changes to the Managed Server Domain Directory"
- Section 9.5.5, "Starting and Validating the WLS_SOAI Managed Server"
- Section 9.5.6, "Propagating the Domain Configuration to SOAHOST2"

9.5.1 Disabling Host Name Verification for the WLS_SOAn Managed Servers

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 Suite. 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 13.3, "Enabling Host Name Verification Certificates for Node Manager" for more information.

To disable host name verification:

1. Log in to WebLogic Server Administration Console.
2. Click Lock & Edit.
3. Expand the Environment node in the Domain Structure window.
4. Click Servers.
5. On the Summary of Servers page, select WLS_SOAI in the Names column of the table.
6. On the settings page for the server, open the SSL tab.
7. Expand the Advanced section of the page.
8. Set host name verification to None.
9. Click Save.
10. Repeat steps 4 through 8 for the WLS_SOAI2 managed server.
11. Save and activate the changes.
12. This change requires a restart of the Administration Server and Node Manager.
   a. To restart the Administration Server see Section 8.4.4, "Starting the Administration Server on SOAHOST1."
   b. To restart Node Manager on SOAHOST1, see Section 9.5.2, "Restarting Node Manager on SOAHOST1."
9.5.2 Restarting Node Manager on SOAHOST1

Use the startNodeManager.sh script to restart Node Manager.

To restart 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 Validating GridLink Data Sources

After you finish configuring WLS_SOA1 and WLS_SOA2 and start the Administration Server and managed servers, verify that every GridLink data source you created is correctly configured and that the Oracle Notification Service (ONS) setup is correct for each data source on each managed server.

To verify the configuration of a GridLink data source for Oracle SOA Suite:

1. Log in to the Weblogic Server Administration Console.
2. In the Domain Structure tree, expand Services, then click Data Sources.
3. Click the name of a GridLink data source that was created.
4. Click the Monitoring tab, and click the name of one of the servers.
5. Click the Testing tab (Figure 9–6), select one of the servers, and click Test Data Source.
Completing Post-Configuration and Verification Tasks

**Figure 9–6 Testing a GridLink Data Source for Oracle SOA Suite**

![Testing a GridLink Data Source for Oracle SOA Suite](image)

The test should be successful if the configuration is correct.

6. Repeat the test for every WebLogic Server instance that uses the GridLink data source.

To verify the configuration of ONS for a GridLink data source for Oracle SOA Suite:

1. Log in to the Weblogic Server Administration Console.
2. In the *Domain Structure* tree, expand *Services*, then click *Data Sources*.
3. Click the name of a GridLink data source that was created.
4. Click the *Monitoring* tab, and click the name of one of the servers.
5. Click the *ONS* tab and then the *Testing* tab (*Figure 9–7*).
6. Select a server, and click *Test ONS*. 
Completing Post-Configuration and Verification Tasks

Figure 9–7  Testing the ONS Configuration for Oracle SOA Suite

The test should be successful if the configuration is correct. If the ONS test fails, verify that the ONS service is running in the Oracle RAC database nodes:

```
[orcl@CUSTDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node CUSTDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node CUSTDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node CUSTDBHOST2
```

```
[orcl@CUSTDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

```
[orcl@CUSTDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: CUSTDBHOST1
ONS daemon is running on node: CUSTDBHOST2
```

7. Repeat the ONS test for every WebLogic Server instance that uses the GridLink data source.
9.5.4 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 the 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=edgdomaintemplateSOA.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=edgdomaintemplateSOA.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.

9.5.5 Starting and Validating the WLS_SOA1 Managed Server

To start the WLS_SOA1 managed server and check that it is configured correctly:

1. Start the WLS_SOA1 managed server using the WebLogic Server Administration Console as follows:
   
   a. 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).
   
   b. Expand the `Environment` node in the Domain Structure window.
   
   c. Choose `Servers`.
   
   d. On the Summary of Servers page, open the `Control` tab.
   
   e. Select `WLS_SOA1` 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 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.
3. Access the following URLs:
   - Access http://SOAHOST1VHN1:8001/wsm-pm to verify the status of Web Services Manager. Click Validate Policy Manager. A list of policies and assertion templates available in the data store opens. The configuration is incorrect if no policies or assertion templates appear.
   - Access http://SOAHOST1VHN1:8001/integration/worklistapp to verify the status of the worklist application.

9.5.6 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 covers the following topics:
- Section 9.5.6.1, "Propagating the Domain Configuration to SOAHOST2 Using the unpack Utility"
- Section 9.5.6.2, "Starting and Validating the WLS_SOA2 Managed Server"

9.5.6.1 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 commands on SOAHOST1 to copy the template file created in the previous step to SOAHOST2:
   ```
   cd ORACLE_BASE/product/fmw/oracle_common/common/bin
   scp edgdomaintemplateSOA.jar oracle@SOAHOST2:
   ORACLE_BASE/product/fmw/oracle_common/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/mserver/domain_name
   -template=edgdomaintemplateSOA.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
   ```

   **Note:** Run unpack from the ORACLE_COMMON_HOME/common/bin directory, not from WL_HOME/common/bin.

   **Note:** The ORACLE_BASE/admin/domain_name/mserver directory must exist before you run unpack. In addition, the ORACLE_BASE/admin/domain_name/mserver/applications directory must be empty.
### 9.5.6.2 Starting and Validating the WLS_SOA2 Managed Server

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

1. Start the WLS_SOA2 managed server using the 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, open the Control tab.
   d. Select WLS_SOA2 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 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

3. Access the following URLs:
   - Access http://SOAHOST2VHN1:8001/wsm-pm to verify the status of Web Services Manager. Click Validate Policy Manager. A list of policies and assertion templates available in the data store opens.
   
   **Note:** The configuration is incorrect if no policies or assertion templates appear.


### 9.6 Configuring the Java Object Cache for Oracle Web Services Manager

The Java Object Cache (JOC) should be configured among all the servers running Oracle Web Services Manager (Oracle WSM). This local cache is provided to increase the performance of Oracle WSM. 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 the configuration of JOC ports for Oracle products, Oracle recommends using ports in the 9988 to 9998 range.

**Note:** After you configure 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/oracle_common/common/bin/wlst.sh
$ connect()
```

Enter the server URL, 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:/domain_name/serverConfig>execfile("MW_HOME/oracle_common/bin/configure-joc.py")
```

Specifically, for enterprise deployment environments, the first cluster option in step 2 should be used. Here is a walkthrough for using configure-joc.py for EDG environments (see below for the script input parameters):

```
Execfile("MW_HOME/oracle_common/bin/configure-joc.py").
Enter Hostnames (eg host1,host2) : SOAHOST1VHN1,SOAHOST2VHN1
.
Do you want to specify a cluster name (y/n) <y> y
.
Enter Cluster Name : SOA_Cluster
.
Enter Discover Port : 9991
.
Do you want to exclude any server(s) from JOC configuration (y/n) <n> n
```

You can also 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*.

**Script Input Parameters**

The input parameters are prompted by the script. The script can be used to perform the following JOC configurations:

- **Configure JOC for all specified 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. For example:

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

- **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>
Enter Managed Server and Discover Port (eg WLS_SOA1:9991, WLS_SOA2:9991) : WLS_SOA1:9999,WLS_SOA2:9999
```
This example configures JOC only for the specified managed servers (that is, WLS_SOA1 and WLS_SOA2). The discover port is specified with the managed server (for example, WLS_SOA1:2222).

- **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_SOA1,WLS_SOA2

- **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`.

### 9.7 Configuring Oracle HTTP Server for the WLS_SOA Managed Servers

To enable Oracle HTTP Server to route to SOA_Cluster, which contain the WLS_SOA 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:

   ```
   # WSM-PM
   <Location /wsm-pm>
   WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
   SetHandler weblogic-handler
   WLProxySSL OFF
   WLProxySSLPassThrough OFF
   </Location>

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

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

   # Worklist
   <Location /integration/>
   WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
   SetHandler weblogic-handler
   WLProxySSL OFF
   WLProxySSLPassThrough OFF
   </Location>
   ```
# UMS prefs

```xml
<Location /sdpmessaging/userprefs-ui>
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

# Default to-do taskflow

```xml
<Location /DefaultToDoTaskFlow/>
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

# Workflow

```xml
<Location /workflow>
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

# SOA Composer

```xml
<Location /soa/composer>
    WebLogicCluster SOAHOST1VHN1:8001,SOAHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

2. **Make sure the httpd.conf file located in the same directory as the mod_wl_ohs file contains the following lines:**

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

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

```xml
NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName soainternal.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>
```
3. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohsX
```

For WEBHOST1, use `ohs1` for `ias-component` and for WEBHOST2 use `ohs2`.

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. Please 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.

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 run time.

- **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*.

### 9.8 Setting the Frontend HTTP Host and Port

You must set the frontend HTTP host and port for the Oracle WebLogic Server cluster hosting the Oracle SOA Suite servers:

1. Log in to WebLogic Server Administration Console.
2. Go to the Change Center section and click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Clusters**.
5. On the Summary of Servers page, select **SOA_Cluster**.
6. Open the **HTTP** tab.
7. Set the following values:
   - **Frontend Host**: soainternal.mycompany.com
   - **Frontend HTTP Port**: 80
8. Click **Save**.

---

**Note:** Values such as `wcc.mycompany.com:443`, `admin.mycompany.com:80` and `you@youraddress` that are noted in this document serve as examples only. Enter values based on the actual environment.
9. Click **Activate Changes** in the Change Center section of the Administration Console.

10. Restart the servers to make the frontend host directive in the cluster take effect.

### 9.9 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as **Running** in the Administration Console. If the server is shown as **Starting** or **Resuming**, wait for the server status to change to **Started**. If another status is reported (such as **Admin** or **Failed**), check the server output log files for errors. See Section 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

Validate WSM_Cluster through Oracle HTTP Server using the following URLs (for both WEBHOST1 and WEBHOST2):

- http://WEBHOSTn:7777/soa-infra
- http://WEBHOSTn:7777/integration/worklistapp
- http://WEBHOSTn:7777/soa/composer
- http://WEBHOSTn:7777/wsm-pm

For information on configuring system access through the load balancer, see Section 3.3, "Configuring the Load Balancer."

---

**Note:** After the registering Oracle HTTP Server as described in Section 8.5.3, "Registering Oracle HTTP Server with WebLogic Server," Oracle HTTP Server should appear as a manageable target in the Oracle Enterprise Manager console. To verify this, log in to the Oracle Enterprise Manager console. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

---

### 9.10 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. Oracle 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 managed 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:

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.
3. On the Summary of Servers page, click the name of the server (represented as a hyperlink) in the Name column of the table. The settings page for the selected server opens and defaults to the **Configuration** tab.
4. Open the Services tab within the Configuration tab (not the top-level Services tab).

5. Click Lock & Edit.

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. Save and activate the changes.

8. Restart the WLS_SOA1 and WLS_SOA2 managed servers.

9.11 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: 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.

Using the Database Mutex Locking Operation

To make an outbound Oracle File or FTP Adapter service highly available using database table as a coordinator, you must modify the Oracle File Adapter deployment descriptor for the connection-instance corresponding to eis/HAFFileAdapter in the Oracle WebLogic Server console.

Note: You must increase global transaction timeouts if you use database as a coordinator.
To use the Database Mutex locking operation:

1. Log in to the Oracle WebLogic Server console. To access the console, navigate to http://server_name:port_number/console.
2. Click Deployments in the left pane for Domain Structure.
3. Click FileAdapter under Summary of Deployments on the right pane.
4. Open the Configuration tab.
5. Open the Outbound Connection Pools tab, and expand javax.resource.cci.ConnectionFactory to see the configured connection factories.
6. Click eis/HAFolder. The Outbound Connection Properties screen for the connection factory corresponding to high availability opens. The connection factory properties are displayed as shown in Figure 9–8.

![Figure 9–8 Oracle WebLogic Server Console - Settings for javax.resource.cci.ConnectionFactory Page](image-url)
7. Click **Lock & Edit**. After this, the property value column becomes editable (you can select any of the rows under **Property Value** and modify its value).

The new parameters in connection factory for Oracle File and FTP Adapters follow:

- **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:

  \texttt{ORACLE\_BASE/admin/domain\_name/cluster\_name/fadapter}

- **inboundDataSource**: Set the value to \texttt{jdbc\_SOADatasource}. This is the data source where the schemas corresponding to high availability are pre-created. The pre-created schemas can be found under \texttt{ORACLE\_HOME/rcu/integration/soainfra/sql/adaptercreateschema\_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 \texttt{jdbc\_SOADatasource}. This is the data source where the schemas corresponding to high availability are pre-created. The pre-created schemas can be found under \texttt{ORACLE\_HOME/rcu/integration/soainfra/sql/adaptercreateschema\_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.

- **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 (\texttt{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 (\texttt{oracle.tip.adapter.file.Mutex}) and then configure a new binding-property with the name \texttt{oracle.tip.adapter.file.mutex} and value as the fully qualified class name for the mutex for the outbound reference.

---

**Note**: The parameters available for FTP Adapters are slightly different than for the connection factory, but from a high-availability standpoint, just setting the control directory to a shared storage location is what matters.

---

8. Click **Save** after you update the properties.

9. On the Save Deployment Plan page, enter a shared storage location for the deployment plan. The directory structure is as follows:

  \texttt{ORACLE\_BASE/admin/domain\_name/cluster\_name/dp/Plan.xml}
10. **Click Save and Activate.**

11. **Configure BPEL Process or Mediator Scenario to use the connection factory as shown in the following example:**

```xml
<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.

### 9.12 Scaling the Oracle Database Adapter

**Note:** this step is optional and applies only to those deployments that require adapter support for the BPEL processes that are invoked by.

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 Oracle Fusion Middleware 11g Release 1 (11.1.2.0), that approach has now been superseded. If you were using this approach previously, you can simply remove (in db.jca) or clear (on the Logical Delete wizard page) the `MarkReservedValue` attribute, and you will 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 non-recoverable situations in high-availability environments is minimized.
- No unique `MarkReservedValue` needs to be specified. Previously, for this to work, you had 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.
9.13 Configuring Node Manager for the WLS_SOA Managed Servers

Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses communicating with the Administration Server and other servers. See Chapter 13, "Setting Up Node Manager" for further details. The procedures in that chapter must be performed twice using the following information:

<table>
<thead>
<tr>
<th>Run</th>
<th>Host Name (HOST)</th>
<th>Virtual IP (VIP)</th>
<th>Server Name (WLS_SERVER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run 1:</td>
<td>SOAHOST1</td>
<td>SOAHOST1VHN1</td>
<td>WLS_SOA1</td>
</tr>
<tr>
<td>Run 2:</td>
<td>SOAHOST2</td>
<td>SOAHOST2VHN1</td>
<td>WLS_SOA2</td>
</tr>
</tbody>
</table>

9.14 Configuring Server Migration for the WLS_SOA Managed Servers

Server migration is required for proper failover of the Oracle SOA Suite components in the event of failure in any of the SOAHOST1 and SOAHOST2 nodes. See Chapter 14, "Configuring Server Migration for an Enterprise Deployment" for further details. For Oracle SOA Suite, use the following values for the variables in that chapter:

- Server names:
  - WLS_SERVER1: WLS_SOA1
  - WLS_SERVER2: WLS_SOA2

- Host names:
  - HOST1: SOAHOST1
  - HOST2: SOAHOST2

- Cluster name:
  - CLUSTER: SOA_Cluster

9.15 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. This backup can be discarded 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 for information on database backup.
To back up the installation at this point:

1. Back up the web tier on WEBHOST1:
   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 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 and managed server domain directories to save your domain configuration. The configuration files all exist in the `ORACLE_BASE/admin/domain_name` directory. Run the following command on SOAHOST1 to create the backup:

   ```
   tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
   ```
Extending the Domain to Include Oracle WebCenter Content

This chapter describes how to extend a domain to include Oracle WebCenter Content using the Oracle Fusion Middleware Configuration Wizard. It contains the following sections:

- Section 10.1, "Overview of Extending the Domain to Include Oracle WebCenter Content"
- Section 10.2, "Enabling WCCHOST1VHN1 on WCCHOST1 and WCCHOST2VHN1 on WCCHOST2"
- Section 10.3, "Extending the Domain to Include WebCenter Content"
- Section 10.4, "Starting Node Manager on WCCHOST1 and WCCHOST2"
- Section 10.5, "Validating GridLink Data Sources for WCC_WLS1"
- Section 10.6, "Propagating the Domain Configuration to the Managed Server Domain Directories"
- Section 10.7, "Restarting the Administration Server"
- Section 10.8, "Starting the WLS_WCC1 Managed Server and Configuring Content Server"
- Section 10.9, "Updating the cwallet File in the Administration Server"
- Section 10.10, "Starting the WLS_WCC2 Managed Server and Configuring Content Server"
- Section 10.11, "Validating GridLink Data Sources for WLS_WCC2"
- Section 10.12, "Configuring Service Retries for Oracle WebCenter Content"
- Section 10.13, "Configuring Oracle HTTP Server for the WLS_WCC Managed Servers"
- Section 10.14, "Validating Access Through Oracle HTTP Server"
- Section 10.15, "Configuring Node Manager for the WLS_WCC and WLS_IMG Managed Servers"
- Section 10.16, "Backing Up the Installation"

Note: Before starting the setup process, read the release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at http://docs.oracle.com/cd/E23943_01/relnotes.htm.
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. WCCHOST1 and WCCHOST2 mount MW_HOME and reuse the existing Oracle Weblogic Server, Oracle SOA Suite, and Oracle WebCenter Content binary installations. The pack and unpack utilities are used to bootstrap the domain configuration for the WLS_WCC1 and WLS_WCC2 servers in these two new nodes. As a result, you do not need to install any software in these two nodes.

For the Oracle WebCenter Content system to work properly, WCCHOST1 and WCCHOST2 must maintain the same system requirements and configuration that was required for installing Oracle Fusion Middleware in SOAHOST1 and SOAHOST2. Otherwise, unpredictable behavior in the execution of binaries may occur.

Note: You will have already added Oracle SOA Suite components to the domain, as described in Section 9, "Extending the Domain to Include Oracle SOA Suite Components."

Extend the domain to include Oracle WebCenter Content. Table 10–1 lists the steps for configuring WebCenter Content and other tasks required for extending the domain with WebCenter Content managed servers.

<table>
<thead>
<tr>
<th>Table 10–1</th>
<th>Steps for Extending the Domain with WebCenter Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>Prepare for extending the domain for WebCenter Content</td>
<td>Enable a VIP mapping for each of the host names.</td>
</tr>
<tr>
<td>Extend the domain for WebCenter Content</td>
<td>Extend the WebLogic Server domain you created in Chapter 8, &quot;Creating a Domain for an Enterprise Deployment.&quot;</td>
</tr>
<tr>
<td>Start Node Manager on the WebCenter Content managed servers</td>
<td>Run the setNMProps.sh script and then start Node Manager on WCCHOST1 and on WCCHOST2.</td>
</tr>
<tr>
<td>Verify the configuration of GridLink data sources and Oracle Notification Service (ONS) for WCC_WLS1</td>
<td>Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.</td>
</tr>
<tr>
<td>Propagate the domain configuration to the WebCenter Content managed servers</td>
<td>Propagate the start scripts and classpath configuration from the Administration Server’s domain directory to the managed server domain directories.</td>
</tr>
<tr>
<td>Restart the Administration Server for the domain</td>
<td>Stop and then restart the Administration Server.</td>
</tr>
<tr>
<td>Start the first WebCenter Content managed server and configure its Content Server instance</td>
<td>Start the WLS_WCC1 managed server and complete the initial Content Server configuration.</td>
</tr>
<tr>
<td>Propagate the changes in the cwallet.sso file back to the Administration Server</td>
<td>Copy the updated cwallet.sso file to the Administration Server directory.</td>
</tr>
</tbody>
</table>
10.2 Enabling WCCHOST1VHN1 on WCCHOST1 and WCCHOST2VHN1 on WCCHOST2

This step is required for server migration of WLS_WCC1 and WLS_WCC2. You will associate the WLS_WCC1 and WLS_WCC2 servers with virtual host names (WCCHOST1VHN1 and WCCHOST2VHN1). Check that these virtual host names are enabled by DNS or /etc/hosts resolution in your system and that they map to the appropriate VIPs).

For more information, see Section 9.2, "Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2."

10.3 Extending the Domain to Include WebCenter Content

You can extend the domain created in Section 8, "Creating a Domain for an Enterprise Deployment" to include Oracle WebCenter Content. The instructions in this section assume that the Oracle WebCenter Content deployment uses the same database service as the Oracle SOA Suite deployment (wccedg.mycompany.com).

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. Make sure that the database where you installed the repository is running.
   For Oracle RAC databases, it is recommended that all instances are running, so that the validation check later on becomes more reliable.

2. On SOAHOST1, change the directory to the location of the Oracle Fusion Middleware Configuration Wizard. This is within the Oracle Common home directory (domain extensions are run from the node where the Administration Server resides).
   
   ```
   cd ORACLE_COMMON_HOME/common/bin
   ```

3. Start the Fusion Middleware Configuration Wizard:
   ```
   ./config.sh
   ```

4. In the Welcome screen, select **Extend an existing WebLogic domain**, and click Next.

5. In the WebLogic Domain Directory screen, select the WebLogic Server domain directory (`ORACLE_BASE/admin/domain_name/aserver/domain_name`), and click Next.

6. In the Select Extension Source screen (Figure 10–1), make these selections:
   - Select **Extend my domain automatically to support the following added products**.
   - Select this product:
     
     Oracle Universal Content Management - Content Server - 11.1.1.0 [wcc]
     This is the selection for Oracle WebCenter Content.
The following products should already be selected and grayed out. They were selected when you created the domain (Section 8.3) or extended it for Oracle SOA Suite components (Section 9.3).

**Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3]**

**Oracle SOA Suite for developers - 11.1.1.0 [soa]**

**Oracle SOA Suite - 11.1.1.0 [soa]**

**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]**

Click Next.

7. In the Configure JDBC Component Schema screen (Figure 10–2), do the following:

a. Select **UCM Schema** (for WebCenter Content). Do not select any of the other existing schemas.
b. For the RAC configuration, you can select **Convert to GridLink** or **Convert to RAC multi data source** (described in **Appendix A, "Using Multi Data Sources with Oracle RAC"**). For the instructions given here, select **Convert to GridLink**.

   After you select a RAC configuration, all selected schemas are grayed.

c. **Click Next.**

8. In the Configure GridLink RAC Component Schema screen (**Figure 10–3**), do the following:

a. Select **UCM Schema** (for WebCenter Content). Leave the other data sources as they are.
b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

- **Driver**: Select Oracle driver (Thin) for GridLinkConnections, Versions: 10 and later.

- **Service Name**: Enter the service name of the Oracle RAC database in lowercase letters, followed by the domain name; for example, wccedg.mycompany.com.

- **Username**: Enter the complete user name for the database schema owner of the corresponding component.

  This book uses DEV as the prefix of user names for the database schemas.

- **Password**: Enter the password for the database schema owner.

- **Select Enable FAN**.

- **Enable SSL**: Leave this option deselected.

  If you select SSL to enable Oracle Notification Service (ONS) notification encryption, provide the appropriate Wallet File and Wallet Password details.

- **Service listener**: Enter the Oracle Single Client Access Name (SCAN) address and port for the Oracle RAC database being used. The protocol should be TCP.
Oracle recommends that you use a SCAN address to specify the Service Listener (and ONS Host) so you do not need to update a GridLink data source containing a SCAN address if you add or remove Oracle RAC nodes. To determine the SCAN address, query the `remote_listener` parameter in the database:

```
SQL> show parameter remote_listener;
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_listener</td>
<td>string</td>
<td>db-scan.mycompany.com:1521</td>
</tr>
</tbody>
</table>

**Note:** For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener; for example:

```
custdbhost1-vip.mycompany.com (port 1521)
```

and

```
custdbhost2-vip.mycompany.com (1521)
```

For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database. For information about configuring multi data sources, see Appendix A, "Using Multi Data Sources with Oracle RAC."

- **ONS Host**: Enter here also the SCAN address for the RAC database and the ONS remote port, as reported by the database:

  ```
  [orcl@CUSTDBHOST2~]$ srvctl config nodeapps -s
  ONS exists: Local port 6100, remote port 6200, EM port 2016
  ```

**Note:** For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service; for example:

```
custdbhost1.mycompany.com (port 6200)
```

and

```
custdbhost2.mycompany.com (6200)
```

c. Click Next.

**Note:** Leave the SOA Infrastructure, User Messaging Service, OWSM MDS Schema, and SOA MDS Schema information as is.

9. In the Test JDBC Component Schema screen (Figure 10-4), select the UCM Schema row, then click Test Connections.

The **Connection Results Log** displays the results. Ensure that the connection to the database that contains the schema was successful. If not, click Previous to return to the previous screen, correct your entry, and then retry the test.
Extending the Domain to Include WebCenter Content

**Figure 10–4  Test JDBC Component Schema Screen for WebCenter Content**

![Test JDBC Component Schema Screen](image)

Click Next when the connection is successful.

10. In the Optional Configuration screen, select the following options:
   - Managed Servers, Clusters and Machines
   - Deployment and Services

   Click Next.

11. In the Configure Managed Servers screen (Figure 10–5), add the required managed servers.
A server is created automatically. Rename this server to WLS_WCC1 and add a new server called WLS_WCC2. Give these servers the attributes listed in Table 10–2. Do not modify the other servers that are shown in this screen; leave them as they are.

12. In the Configure Clusters screen (Figure 10–6, click Add to add the clusters as shown in Table 10–3. Do not modify the other clusters that appear in this screen; leave them as they are.

Table 10–2 Managed Servers

<table>
<thead>
<tr>
<th>Name</th>
<th>Listen Address</th>
<th>Listen Port</th>
<th>SSL Listen Port</th>
<th>SSL Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLS_WCC1</td>
<td>WCCHOST1</td>
<td>16200</td>
<td>n/a</td>
<td>No</td>
</tr>
<tr>
<td>WLS_WCC2</td>
<td>WCCHOST2</td>
<td>16200</td>
<td>n/a</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 10–3 Clusters

<table>
<thead>
<tr>
<th>Name</th>
<th>Cluster Messaging Mode</th>
<th>Multicast Address</th>
<th>Multicast Port</th>
<th>Cluster Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCC_Cluster</td>
<td>unicast</td>
<td>n/a</td>
<td>n/a</td>
<td>Leave empty</td>
</tr>
</tbody>
</table>
Extending the Domain to Include Oracle WebCenter Content

Figure 10–6 Configure Clusters Screen for WebCenter Content

Click Next.

13. 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.

14. In the Configure Machines screen (Figure 10–7), open the Unix Machine tab and add the following two new machines:

<table>
<thead>
<tr>
<th>Table 10–4 Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>WCCHOST1</td>
</tr>
<tr>
<td>WCCHOST2</td>
</tr>
</tbody>
</table>

Leave all other fields to their default values.
Click **Next**.

15. In the Assign Servers to Machines screen (**Figure 10–8**), assign servers to machines as follows:
   - Assign `WLS_WCC1` to `WCCHOST1`.
   - Assign `WLS_WCC2` to `WCCHOST2`.
16. In the Target Deployments to Clusters or Servers screen, make sure that the DMS Application is targeted to the SOA_Cluster, WCC_Cluster and Admin Server. Click Next.

17. In the Target Services to Clusters or Servers screen, click Next.

18. In the Configuration Summary screen, click Extend.

19. If you see a warning dialog about port conflicts for the domain, click OK.

20. In the Creating Domain screen, click Done.

21. Restart the Administration Server to make these changes to take effect. See Section 10.7, "Restarting the Administration Server."
10.4 Starting Node Manager on WCCHOST1 and WCCHOST2

To start Node Manager on WCCHOST1 and WCCHOST2 if Node Manager has not started already:

1. On both WCCHOST1 and WCCHOST2, 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. See also Section 16.11.3, "Incomplete Policy Migration After Failed Restart of SOA Server."

2. Run the following commands on both WCCHOST1 and WCCHOST2 to start Node Manager:

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

10.5 Validating GridLink Data Sources for WCC_WLS1

Before you propagate the domain configuration to WCCHOST2, verify that every GridLink data source you created is correctly configured and that the Oracle Notification Service (ONS) setup is correct for each data source on each managed server.

To verify the configuration of a GridLink data source for WebCenter Content:

1. Log in to the Weblogic Server Administration Console.
2. In the Domain Structure tree, expand Services, then click Data Sources.
3. Click the name of a GridLink data source that was created.
4. Click the Monitoring tab, and click the name of one of the servers.
5. Click the Testing tab (Figure 10–9), select one of the servers, and click Test Data Source.
Validating GridLink Data Sources for WCC_WLS1

Extending the Domain to Include Oracle WebCenter Content

Figure 10–9 Testing a GridLink Data Source for WebCenter Content

The test should be successful if the configuration is correct.

6. Repeat the test for every WebLogic Server instance that uses the GridLink data source.

To verify the configuration of ONS for a GridLink data source for WebCenter Content:

1. Log in to the Weblogic Server Administration Console.

2. In the Domain Structure tree, expand Services, then click Data Sources.

3. Click the name of a GridLink data source.

4. Click the ONS tab and then the Testing tab (Figure 10–10).

5. Select a server, and click Test ONS.
The test should be successful if the configuration is correct. If the ONS test fails, verify that the ONS service is running in the Oracle RAC database nodes:

```bash
[orcl@CUSTDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node CUSTDBHOST1
SCAN listener LISTENER_SCAN2 is enabled
SCAN Listener LISTENER_SCAN2 is running on node CUSTDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node CUSTDBHOST2
```

```bash
[orcl@CUSTDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

```bash
[orcl@CUSTDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: CUSTDBHOST1
ONS daemon is running on node: CUSTDBHOST2
```

6. Repeat the ONS test for every WebLogic Server instance that uses the GridLink data source.
10.6 Propagating the Domain Configuration to the Managed Server

Domain Directories

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=edgdomaintemplateWCC.jar -template_name=edgdomain_templateWCC
   ```

2. Run the following command on SOAHOST1 to copy the template pack created in the previous step to WCCHOST2:

   ```
   scp edgdomaintemplateWCC.jar oracle@WCCHOST2:ORACLE_BASE/product/fmw/oracle_common/common/bin
   ```

3. Run the unpack command on WCCHOST1 to unpack the propagated template.

   ```
   cd ORACLE_COMMON_HOME/common/bin
   
   ./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template=edgdomaintemplateWCC.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
   ```

   **Note:** Make sure to run unpack from the ORACLE_COMMON_HOME/common/bin directory, not from WL_HOME/common/bin.

4. Repeat step 3 for WCCHOST2.

10.7 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 8.4.4, "Starting the Administration Server on SOAHOST1."
10.8 Starting the WLS_WCC1 Managed Server and Configuring Content Server

After you start the WLS_WCC1 managed server, you can configure Oracle WebCenter Content Server through the web interface.

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, open 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 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

Configuring Content Server
To configure Content Server:

1. Log in to WLS_WCC1 at http://WCCHOST1:16200/cs using your WebLogic Server 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 of the Oracle WebCenter Content enterprise deployment is at ORACLE_BASE/admin/domain_name/wcc_cluster_name.

2. Change the following values on the server configuration page (make sure to select the Is New Content Server Instance checkbox to see all options):

   - **Content Server Instance Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs.
   - **Native File Repository Location**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/vault.
   - **WebLayout Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/weblayout.
   - **User Profile Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/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|WCCHOST1|WCCHOST2|WEBHOST1|WEBHOST2
Starting the WLS_WCC2 Managed Server and Configuring Content Server

1. WebServer HTTP/HTTPS Address: Set this to wcc.mycompany.com:443.
2. Web Address is HTTPS: Select this checkbox.
3. Server Instance Label: Set this to WCC_Cluster1.
4. Server Instance Description: Set this to Cluster wcc_cluster1.
5. Auto_Number Prefix: Set this to wcc_cluster1-.

3. Click Submit when finished, and restart the managed server using the WebLogic Server Administration Console.

10.9 Updating the cwallet File in the Administration Server

Oracle WebCenter Content Server updates the cwallet.sso file located in ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig when it starts. This change needs to be propagated back to the Administration Server. To do this, copy the file to ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig on SOAHOST1 using the following command on WCCHOST1 (all on a single line):

```
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 servers that modifies the cwallet.sso file in the ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig directory, the file will have to be immediately copied to the Administration Server domain directory on SOAHOST1 at ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig.

10.10 Starting the WLS_WCC2 Managed Server and Configuring Content Server

After you start the WLS_WCC2 managed server, you can configure Oracle WebCenter Content Server through the web interface.
Starting the WLS_WCC2 Managed Server

To start the WLS_WCC2 managed server:

1. Start the WLS_WCC2 managed server using the 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, open 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 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

Configuring Content Server

To configure Content Server:

1. Log in to WLS_WCC2 at http://WCCHOST2:16200/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 of the Oracle WebCenter Content enterprise deployment is at ORACLE_BASE/admin/domain_name/wcc_cluster_name.

2. Change the following values on the server configuration page:
   - **Content Server Instance Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs.
   - **Native File Repository Location**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/vault.
   - **WebLayout Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/weblayout.
   - **User Profile Folder**: Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/data/users/profiles.

   Make sure that the **Is new Content Server Instance?** checkbox is not selected.

3. Click Submit when finished and restart the managed server using the WebLogic Server Administration Console.
10.11 Validating GridLink Data Sources for WLS_WCC2

After you finish configuring WLS_WCC1 and WLS_WCC2 and start the Administration Server and managed servers, verify that every GridLink data source you created is correctly configured and that the Oracle Notification Service (ONS) setup is correct for each data source on each managed server.

**Note:** To verify that the GridLink data source you created is correctly configured, follow instructions given in Section 10.5, "Validating GridLink Data Sources for WCC_WLS1," but now for second server, WLS_WCC2.

10.12 Configuring Service Retries for Oracle WebCenter Content

The following parameter should be set in the Content Server config.cfg file to enable login retries during an Oracle RAC failover:

```
ServiceAllowRetry=true
```

If this value is not set, users will need to manually retry any operation that was in progress when the failover began.

To add the configuration parameter for Oracle WebCenter Content:

1. Go to Oracle WebCenter Content Server at http://WCCHOST1:16200/cs, and log in using your Oracle WebLogic Server 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.

**Note:** The new parameter is included in the config.cfg file, which is at the following location:

```
ORACLE_BASE/admin/domain_name/wcc_cluster_name/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.)
### 10.13 Configuring Oracle HTTP Server for the WLS_WCC Managed Servers

To enable Oracle HTTP Server to route to WCC_Cluster, which contain 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:

   ```
   # UCM
   <Location /cs>
     WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
     SetHandler weblogic-handler
     WLCookieName JSESSIONID
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>
   
   <Location /adfAuthentication>
     WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
     SetHandler weblogic-handler
     WLCookieName JSESSIONID
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>
   
   <Location /_ocsh>
     WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
     SetHandler weblogic-handler
     WLCookieName JSESSIONID
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>
   ```

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

   ```
   ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohsX
   
   For WEBHOST1, use ohs1 for ias-component and for WEBHOST2 use ohs2.
   ```

### 10.14 Validating Access Through Oracle HTTP Server

You should verify URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCC_Cluster. To verify the URLs:

1. While WLS_WCC2 is running, stop WLS_WCC1 using the WebLogic Server Administration Console.
2. Access http://WEBHOST1:7777/cs to verify it is functioning properly.
3. Start WLS_WCC1 from the WebLogic Server Administration Console.
4. Stop WLS_WCC2 from the WebLogic Server Administration Console.
5. Access http://WEBHOST1:7777/cs to verify it is functioning properly.
### 10.15 Configuring Node Manager for the WLS_WCC and WLS_IMG Managed Servers

Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses communicating with the Administration Server and other servers. See Chapter 13, "Setting Up Node Manager" for further details. The procedures in that chapter must be performed twice using the following information:

<table>
<thead>
<tr>
<th>Run</th>
<th>Host Name (HOST)</th>
<th>Virtual IP (VIP)</th>
<th>Server Name (WLS_SERVER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run 1:</td>
<td>WCCHOST1</td>
<td>WCCHOST1VHN1</td>
<td>WLS_WCC1</td>
</tr>
<tr>
<td>Run 2:</td>
<td>WCCHOST2</td>
<td>WCCHOST2VHN1</td>
<td>WLS_WCC2</td>
</tr>
</tbody>
</table>

* Optional; required only for Oracle WebCenter Content: Imaging managed servers (WLS_IMG).

Please note the following:

- Even though the WLS_IMG managed servers are not yet configured at this point (see Chapter 11, "Extending the Domain to Include Imaging") and are not mandatory for an Oracle WebCenter Content configuration that includes only WebCenter Content, the virtual host names used by Oracle WebCenter Content: Imaging are configured here to provide a one-step configuration process that includes both types of servers.

- Perform all steps in Chapter 13, "Setting Up Node Manager" except for Section 13.3.5, "Configuring Managed Servers to Use the Custom Keystores" for the WLS_IMG servers. This step can be done after the WLS_IMG servers are added to the domain.
10.16 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. This backup can be discarded 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 for information on database backup.

To back up the installation at this point:

1. Back up the web tier on WEBHOST1:
   a. Shut down the instance using opmnctl.
      
      \[ \text{ORACLE\_BASE/admin/instance\_name/bin/opmnctl stopall} \]
   b. Back up the Middleware Home on the web tier using the following command (as root):
      
      \[ \text{tar -cvpf BACKUP\_LOCATION/web.tar \ MW\_HOME} \]
   c. Back up the Oracle instance on the web tier using the following command:
      
      \[ \text{tar -cvpf BACKUP\_LOCATION/web_instance\_name.tar \ ORACLE\_INSTANCE} \]
   d. Start the instance using opmnctl:
      
      \[ \text{cd ORACLE\_BASE/admin/instance\_name/bin} \]
      \[ \text{opmnctl startall} \]

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 and managed 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 on SOAHOST1 to create the backup:

      \[ \text{tar -cvpf edgdomainback.tar \ ORACLE\_BASE/admin/domain\_name} \]
This chapter describes how to extend a domain with Oracle WebCenter Content: Imaging using the Oracle Fusion Middleware Configuration Wizard. It contains the following sections:

- Section 11.1, "Overview of Extending the Domain for Imaging"
- Section 11.2, "Enabling VIP4 and VIP5 in WCCHOST1 and WCCHOST2"
- Section 11.3, "Extending the Domain to Include Imaging"
- Section 11.4, "Disabling Host Name Verification for the WLS_IMG Managed Servers"
- Section 11.5, "Starting Node Manager on WCCHOST1 and WCCHOST2"
- Section 11.6, "Validating GridLink Data Sources for WCC_IMG1"
- Section 11.7, "Propagating the Domain Configuration to the Managed Server Domain Directories"
- Section 11.8, "Configuring a JMS Persistence Store for Oracle WebCenter Content: Imaging"
- Section 11.9, "Configuring a Default Persistence Store for Transaction Recovery"
- Section 11.10, "Restarting the Administration Server"
- Section 11.11, "Starting the Imaging Managed Servers"
- Section 11.12, "Validating GridLink Data Sources for WLS_IMG2"
- Section 11.13, "Configuring System MBeans for Oracle WebCenter Content: Imaging"
- Section 11.14, "Enabling the Imaging Feature Set in Oracle WebCenter Content"
- Section 11.15, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"
- Section 11.16, "Creating a Connection to Oracle WebCenter Content"
- Section 11.17, "Configuring BPEL CSF Credentials"
- Section 11.18, "Configuring a Workflow Connection"
- Section 11.19, "Configuring Oracle HTTP Server for the WLS_IMG Managed Servers"
- Section 11.20, "Setting the Frontend HTTP Host and Port"
- Section 11.21, "Validating Access Through Oracle HTTP Server"
- Section 11.22, "Configuring Node Manager for the WLS_IMG Managed Servers"
11.1 Overview of Extending the Domain for Imaging

The Oracle WebCenter Content: Imaging 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. WCCHOST1 and WCCHOST2 mount MW_HOME and reuse the existing Oracle WebLogic Server, Oracle SOA Suite, and Oracle WebCenter Content binary installations. The pack and unpack utilities are used to bootstrap the domain configuration for the WLS_IMG1 and WLS_IMG2 servers in these two new nodes. As a result, you do not need to install any software in these two nodes. For the Imaging system to work properly, WCCHOST1 and WCCHOST2 must maintain the same system requirements and configuration that was required for installing Oracle Fusion Middleware in SOAHOST1 and SOAHOST2. Otherwise, unpredictable behavior in the execution of binaries may occur.

Extend the domain to include Imaging. Table 11–1 lists the steps for configuring Imaging and other tasks required for extending the domain with Imaging managed servers.

Table 11–1  Steps for Extending the Domain with Imaging

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for extending the domain for Imaging</td>
<td>Enable a VIP mapping for each of the host names.</td>
<td>Section 11.2, &quot;Enabling VIP4 and VIP5 in WCCHOST1 and WCCHOST2&quot;</td>
</tr>
<tr>
<td>Extend the domain for Imaging</td>
<td>Extend the Imaging domain you created in Chapter 8, &quot;Creating a Domain for an Enterprise Deployment.&quot;</td>
<td>Section 11.3, &quot;Extending the Domain to Include Imaging&quot;</td>
</tr>
<tr>
<td>Disable host name verification for Imaging</td>
<td>Disable host name verification while setting up and validating the topology.</td>
<td>Section 11.4, &quot;Disabling Host Name Verification for the WLS_IMG Managed Servers&quot;</td>
</tr>
<tr>
<td>Start Node Manager on the WebCenter Content managed servers</td>
<td>Run the setNMProps.sh script and then start Node Manager on WCCHOST1 and on WCCHOST2.</td>
<td>Section 11.5, &quot;Starting Node Manager on WCCHOST1 and WCCHOST2&quot;</td>
</tr>
<tr>
<td>Verify the configuration of GridLink data sources and Oracle Notification Service (ONS)</td>
<td>Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.</td>
<td>Section 11.6, &quot;Validating GridLink Data Sources for WCC_IMG1&quot;</td>
</tr>
<tr>
<td>Propagate the domain configuration to the Imaging managed servers</td>
<td>Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the managed server domain directories.</td>
<td>Section 11.7, &quot;Propagating the Domain Configuration to the Managed Server Domain Directories&quot;</td>
</tr>
<tr>
<td>Configure a JMS persistence store</td>
<td>Configure the location for the JMS persistence stores as a directory that is visible to both Imaging managed servers.</td>
<td>Section 11.8, &quot;Configuring a JMS Persistence Store for Oracle WebCenter Content: Imaging&quot;</td>
</tr>
</tbody>
</table>
### Table 11–1 (Cont.) Steps for Extending the Domain with Imaging

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a default persistence store</td>
<td>Configure a default persistence store for transaction recovery.</td>
<td>Section 11.9, &quot;Configuring a Default Persistence Store for Transaction Recovery&quot;</td>
</tr>
<tr>
<td>Restart the Administration Server for the domain</td>
<td>Stop and then restart the Administration Server.</td>
<td>Section 11.10, &quot;Restarting the Administration Server&quot;</td>
</tr>
<tr>
<td>Start the Imaging managed servers</td>
<td>Start the WLS_IMG1 and WLS_IMG2 managed servers.</td>
<td>Section 11.11, &quot;Starting the Imaging Managed Servers&quot;</td>
</tr>
<tr>
<td>Configure System MBeans for Imaging</td>
<td>Configure the <code>InputDirectories</code>, <code>SampleDirectory</code>, and <code>GDFontPath</code> MBeans in the System MBean Browser.</td>
<td>Section 11.13, &quot;Configuring System MBeans for Oracle WebCenter Content: Imaging&quot;</td>
</tr>
<tr>
<td>Enable the Imaging feature set in WebCenter Content</td>
<td>Enable the <code>IpmRepository</code> component of Content Server.</td>
<td>Section 11.14, &quot;Enabling the Imaging Feature Set in Oracle WebCenter Content&quot;</td>
</tr>
<tr>
<td>Add the listen addresses for the Imaging managed servers</td>
<td>Add the host names of the WLS_IMG1 and WLS_IMG2 managed servers (WCCHOST1VHN1 and WCCHOST2VHN1) to the <code>SocketHostNameSecurityFilter</code> parameter list.</td>
<td>Section 11.15, &quot;Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content&quot;</td>
</tr>
<tr>
<td>Create a connection between Imaging and Oracle WebCenter Content</td>
<td>Create a connection to Oracle WebCenter Content Server.</td>
<td>Section 11.16, &quot;Creating a Connection to Oracle WebCenter Content&quot;</td>
</tr>
<tr>
<td>Configure the BPEL CSF credentials</td>
<td>Configure the required credentials to communicate with Oracle SOA Suite</td>
<td>Section 11.17, &quot;Configuring BPEL CSF Credentials&quot;</td>
</tr>
<tr>
<td>Configure a workflow connection for Imaging</td>
<td>Create and test a workflow connection.</td>
<td>Section 11.18, &quot;Configuring a Workflow Connection&quot;</td>
</tr>
<tr>
<td>Configure Oracle HTTP Server with the extended domain</td>
<td>Configure the Oracle HTTP Server with the managed servers, and set the WLS Cluster address for IMG_Cluster.</td>
<td>Section 11.19, &quot;Configuring Oracle HTTP Server for the WLS_IMG Managed Servers&quot;</td>
</tr>
<tr>
<td>Set the front end HTTP host and port for Imaging</td>
<td>Configure the front end HTTP host and port for IMG_Cluster.</td>
<td>Section 11.20, &quot;Setting the Frontend HTTP Host and Port&quot;</td>
</tr>
<tr>
<td>Validate access to WebCenter Content through Oracle HTTP Server</td>
<td>Verify the URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to IMG_Cluster.</td>
<td>Section 11.21, &quot;Validating Access Through Oracle HTTP Server&quot;</td>
</tr>
<tr>
<td>Configure the Imaging managed servers to use custom key stores</td>
<td>Configure Node Manager with the custom key stores for Imaging.</td>
<td>Section 11.22, &quot;Configuring Node Manager for the WLS_IMG Managed Servers&quot;</td>
</tr>
<tr>
<td>Configure server migration for the Imaging managed servers</td>
<td>Specify the Imaging managed server names, host names, and cluster name for migration.</td>
<td>Section 11.23, &quot;Configuring Server Migration for the WLS_IMG Managed Servers&quot;</td>
</tr>
<tr>
<td>Back Up the Imaging Configuration</td>
<td>Back up the newly extended domain configuration.</td>
<td>Section 11.24, &quot;Backing Up the Installation&quot;</td>
</tr>
</tbody>
</table>
11.2 Enabling VIP4 and VIP5 in WCCHOST1 and WCCHOST2

The Oracle WebCenter Content: Imaging system uses a virtual host name as the listen addresses for the managed server on which it is running. These virtual host names and corresponding virtual IPs are required to enable server migration for the Oracle WebCenter Content: Imaging component. You must enable a VIP (VIP4/VIP5) mapping to WCCHOST1VHN1 on WCCHOST1 and WCCHOST2VHN1 on WCCHOST2, and must also correctly resolve the host names in the network system used by the topology (either by DNS Server or hosts resolution).

To enable the VIPs, follow the example described in Section 9.2, "Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2."

11.3 Extending the Domain to Include Imaging

You extend the domain configured in Chapter 10, "Extending the Domain to Include Oracle WebCenter Content" to include Oracle WebCenter Content: Imaging. The instructions in this section assume that the Imaging deployment uses the same database service as the Oracle WebCenter Content deployment (wccedg.mycompany.com). However, a deployment can choose to use a different database service specifically for Imaging.

---

**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: Imaging:

1. Make sure that the database where you installed the repository is running.
   - For Oracle RAC databases, it is recommended that all instances are running, so that the validation check later on becomes more reliable.

2. On SOAHOST1, change the directory to the location of the Fusion Middleware Configuration Wizard. This is within the Oracle Common home directory (domain extensions are run from the node where the Administration Server resides).
   ```
   cd ORACLE_COMMON_HOME/common/bin
   ```

3. Start the Fusion Middleware Configuration Wizard:
   ```
   ./config.sh
   ```

4. In the Welcome screen, select **Extend an existing WebLogic domain**, and click Next.

5. In the WebLogic Domain Directory screen, select the WebLogic Server domain directory (ORACLE_BASE/admin/domain_name/aserver/domain_name), and click Next.

6. In the Select Extension Source screen (Figure 11–1), make these selections:
   - Select **Extend my domain automatically to support the following added products**.
   - Select this product:
     Oracle WebCenter Content: Imaging - 11.1.1.0 [wcc]
The following products should already be selected and grayed out. They were selected when you created the domain (Section 8.3) or extended it for Oracle SOA Suite components (Section 9.3) or WebCenter Content (Section 10.3).

- Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3]
- Oracle SOA Suite for developers - 11.1.1.0 [soa]
- Oracle SOA Suite - 11.1.1.0 [soa]
- Oracle Universal Content Management - Content Server - 11.1.1.0 [wcc]
- 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]

**Figure 11–1 Select Extension Source Screen for Imaging**

Click Next.

7. In the Configure JDBC Component Schema screen, which Figure 11–2 shows, do the following:
   a. Select IPM Schema only (for Imaging). Do not select any of the other existing schemas.
   b. For the RAC configuration, you can select Convert to GridLink or Convert to RAC multi data source (described in Appendix A, "Using Multi Data Sources with Oracle RAC"). For the instructions given here, select Convert to GridLink.

After you select a RAC configuration, all selected schemas are grayed.
c. Click Next.

8. In the Configure GridLink RAC Component Schema screen (Figure 11–3), do the following:
   a. Select IPM Schema (for Imaging). Leave the other data sources as they are.
b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

- **Driver**: Select Oracle driver (Thin) for GridLinkConnections, Versions:10 and later.
- **Service Name**: Enter the service name of the Oracle RAC database in lowercase letters, followed by the domain name; for example, wccedg.mycompany.com.
- **Username**: Enter the complete user name for the database schema owner of the corresponding component.
  This book uses DEV as the prefix of user names for the database schemas.
- **Password**: Enter the password for the database schema owner.
- **Select Enable FAN**.
- **Enable SSL**: Leave this option deselected.
  If you select SSL to enable Oracle Notification Service (ONS) notification encryption, provide the appropriate Wallet File and Wallet Password details.
- **Service listener**: Enter the Oracle Single Client Access Name (SCAN) address and port for the Oracle RAC database being used. The protocol should be TCP.
Oracle recommends that you use a SCAN address to specify the Service Listener (and ONS Host) so you do not need to update a GridLink data source containing a SCAN address if you add or remove Oracle RAC nodes. To determine the SCAN address, query the remote_listener parameter in the database:

```
SQL> show parameter remote_listener;
NAME        TYPE    VALUE
-----------  -------  --------
remote_listener string  db-scan.mycompany.com :1521
```

**Note:** For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener; for example:

custdbhost1-vip.mycompany.com (port 1521)

and

custdbhost2-vip.mycompany.com (1521)

For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database. For information about configuring multi data sources, see Appendix A, "Using Multi Data Sources with Oracle RAC."

- **ONS Host:** Enter here also the SCAN address for the RAC database and the ONS remote port, as reported by the database:

```
[orcl@CUSTDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

**Note:** For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service; for example:

custdbhost1.mycompany.com (port 6200)

and

custdbhost2.mycompany.com (6200)

c. **Click Next.**

**Note:** Leave the UCM Schema, SOA Infrastructure, User Messaging Service, OWSM MDS Schema, and SOA MDS Schema information as is.
9. In the Test JDBC Component Schema screen, select the IPM Schema row, then click Test Connections.

The Connection Results Log displays the results. Ensure that the connection to the database that contains the schema was successful. If not, click Previous to return to the previous screen, correct your entry, and then retry the test.

**Figure 11-4**

![Test JDBC Component Schema](image)

Click Next when the connection is successful.

10. In the Optional Configuration screen, select the following options:

- JMS Distributed Destination
- Managed Servers, Clusters and Machines
- Deployment and Services

Click Next.

11. In the Select JMS Distributed Destination Type screen, select UDD from the drop-down list for the JMS modules of all Oracle Fusion Middleware components. Click Next.

If an override warning appears, click OK to acknowledge it.

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

A server is created automatically. Rename this to WLS_IMG1 and add a new server called WLS_IMG2. Give these servers the attributes listed in Table 11-2. Do not modify the other servers that appear in this screen; leave them as they are.
Extending the Domain to Include Imaging

11-10
Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Content

Click Next.

13. In the Configure Clusters screen, click Add to add the clusters as shown in Table 11–3. Do not modify the other clusters that appear in this screen; leave them as they are.

Table 11–3 Clusters

<table>
<thead>
<tr>
<th>Name</th>
<th>Cluster Messaging Mode</th>
<th>Multicast Address</th>
<th>Multicast Port</th>
<th>Cluster Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMG_Cluster</td>
<td>unicast</td>
<td>n/a</td>
<td>n/a</td>
<td>Leave empty</td>
</tr>
</tbody>
</table>

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.

- **IMG_Cluster**:
  - WLS_IMG1
  - WLS_IMG2

Click Next.

15. In the Configure Machines screen, open the Unix Machine tab. You should see the WCCHOST1 and WCCHOST2 machines and have the following entries:

Table 11–4 Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Node Manager Listen Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAHOST1</td>
<td>SOAHOST1</td>
</tr>
<tr>
<td>SOAHOST2</td>
<td>SOAHOST2</td>
</tr>
<tr>
<td>ADMINVHN</td>
<td>localhost</td>
</tr>
<tr>
<td>WCCHOST1</td>
<td>WCCHOST1</td>
</tr>
<tr>
<td>WCCHOST2</td>
<td>WCCHOST2</td>
</tr>
</tbody>
</table>

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_IMG1** to **WCCHOST1**.
- Assign **WLS_IMG2** to **WCCHOST2**.

Click Next.
17. 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.*, and oracle.soa.* deployments should be targeted to SOA_Cluster only, except for the oracle.soa.workflow.wc library, which should be targeted to both the SOA_Cluster and the IMG_Cluster.

   Click Next.

18. In the Target Service to Cluster or Servers screen, click Next.

19. In the Configuration Summary screen, click Extend.

20. If a dialog window appears warning about conflicts in ports for the domain, click OK. This should be due to pre-existing servers in the nodes and the warning can be ignored.

21. In the Creating Domain screen, click Done.

22. Restart the Administration Server to make these changes to take effect. See Section 11.10, "Restarting the Administration Server."

11.4 Disabling Host Name Verification for the WLS_IMG Managed Servers

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 13, "Setting Up Node Manager"). If you have not configured the server certificates, you will receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the EDG topology configuration is complete, as described in Chapter 13, "Setting Up Node Manager."

To disable host name verification:

1. Log in to WebLogic Server Administration Console.
2. In the Administration Console, select WLS_IMG1, then SSL, and then Advanced.
3. Click Lock & Edit.
4. Set host name verification to None.
5. In the Administration Console, select WLS_IMG2, then SSL, and then Advanced.
6. Set host name verification to None.
7. Save and activate the changes.
### 11.5 Starting Node Manager on WCCHOST1 and WCCHOST2

To start Node Manager on WCCHOST1 and WCCHOST2 if Node Manager has not started already:

1. On both WEBHOST1 and WEBHOST2, 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. See also Section 16.11.3, "Incomplete Policy Migration After Failed Restart of SOA Server."

2. Run the following commands on both WCCHOST1 and WCCHOST2 to start Node Manager:

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

### 11.6 Validating GridLink Data Sources for WCC_IMG1

Before you propagate the domain configuration to WCCHOST2, verify that every GridLink data source you created is correctly configured and that the Oracle Notification Service (ONS) setup is correct for each data source on each managed server.

**To verify the configuration of a GridLink data source for Imaging:**

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure tree, expand Services, then click Data Sources.
3. Click the name of a GridLink data source that was created.
4. Click the Monitoring tab, and click the name of one of the servers.
5. Click the Testing tab (Figure 11–5), select one of the servers, and click Test Data Source.
6. Repeat the test for every WebLogic Server instance that uses the GridLink data source.

To verify the configuration of ONS for a GridLink data source for Imaging:

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure tree, expand Services, then click Data Sources.
3. Click the name of a GridLink data source.
4. Click the ONS tab and then the Testing tab (Figure 11–6).
5. Select a server, and click Test ONS.

The test should be successful if the configuration is correct.
The test should be successful if the configuration is correct. If the ONS test fails, verify that the ONS service is running in the Oracle RAC database nodes:

```
[orcl@CUSTDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node CUSTDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node CUSTDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node CUSTDBHOST2
```

```
[orcl@CUSTDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

```
[orcl@CUSTDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: CUSTDBHOST1
ONS daemon is running on node: CUSTDBHOST2
```

6. Repeat the ONS test for every WebLogic Server instance that uses the GridLink data source.
11.7 Propagating the Domain Configuration to the Managed Server Domain Directories

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/asmserver/domain_name -template=edgdomaintemplateIMG.jar -template_name=edgdomain_templateIMG
   ``

2. Run the following command on SOAHOST1 to copy the template pack created in the previous step to WCCHOST2:

   ```
   scp edgdomaintemplateIMG.jar oracle@WCCHOST2:/ORACLE_BASE/product/fmw/oracle_common/common/bin
   ``

3. Run the `unpack` command on WCCHOST1 to unpack the propagated template.

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template=edgdomaintemplateIMG.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications -overwrite_domain=true
   ``

   **Note:** Make sure to run `unpack` from the `ORACLE_COMMON_HOME/common/bin` directory, not from `WL_HOME/common/bin`.

4. Repeat step 3 for WCCHOST2.

11.8 Configuring a JMS Persistence Store for Oracle WebCenter Content: Imaging

Configure the location for the JMS persistence stores as a directory that is visible from both nodes. By default, the JMS servers used by Oracle WebCenter Content: Imaging are configured with no persistence store and use the Oracle WebLogic Server store (`ORACLE_BASE/admin/domain_name/mserver/domain_name/servers/server_name/data/store/default`). You must change the Imaging JMS server persistence store to use a shared base directory as follows:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the Services node and then click the Persistence Stores node.
4. Click New, and then Create File Store.
5. Enter a name (for example, IMGJMSServer1Store, which allows you identify the service it is created for) and target WLS_IMG1. Enter a directory that is located in shared storage so that it is accessible from both WCCHOST1 and WCCHOST2 (ORACLE_BASE/admin/domain_name/img_cluster_name/jms).
6. Click OK and activate the changes.
7. In the Domain Structure window, expand the Services node and then click the Messaging->JMS Servers node.
8. On the Summary of JMS Servers page, click the IpmJmsServer1 JMS Server (represented as a hyperlink) from the Name column of the table.
10. In the Persistent Store drop-down list, select IMGJMSServer1Store.
11. Click Save and Activate.
12. Repeat the steps and create IMGJMSServer2Store for IMGJMSServer2.

11.9 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log which stores information about committed transactions that are coordinated by the server that may not have been completed. Oracle 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 the server.

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 for WLS_IMG1:

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure window, expand the Environment node and then click the Servers node.
3. On the Summary of Servers page, click WLS_IMG1 (represented as a hyperlink) in the Name column of the table. The settings page for the WLS_IMG1 server opens with the Configuration tab active.
4. Open the Services tab.
5. Click Lock & Edit.
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/img_cluster_name/tlogs
7. Click **Save** and activate the changes.
8. Repeat the step for the WLS_IMG2 server.

---

**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 WCCHOST1 and WCCHOST2 must be able to access this directory. This directory must also exist before you restart the server.

---

### 11.10 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 8.4.4, "Starting the Administration Server on SOAHOST1."

### 11.11 Starting the Imaging Managed Servers

To start the WLS_IMG1 managed server on WCCHOST1:

1. Start the WLS_IMG1 managed server:
   b. In the Domain Structure window, expand the **Environment** node and then select **Servers**.
   c. On the Summary of Servers page, open the **Control** tab.
   d. Select WLS_IMG1 from the **Servers** column of the table.
   e. Click **Start**.

2. Access http://WCCHOST1VHN1:16000/imaging to verify the status of WLS_IMG1. The Oracle WebCenter Content: Imaging login page appears. Enter your Oracle WebLogic Server administration user name and password to log in. Verify that the PROCESSES initialization parameter for the database is set to a high enough value. See Section 5.2.3, "Initialization Parameters" for details. This error often occurs when you start servers that are subsequent to the first server.

3. Start the WLS_IMG2 managed server:
   b. In the Domain Structure window, expand the **Environment** node and then select **Servers**.
   c. On the Summary of Servers page, open the **Control** tab.
   d. Select WLS_IMG2 from the **Servers** column of the table.
   e. Click **Start**.

4. Access http://WCCHOST2VHN1:16000/imaging to verify the status of WLS_IMG2. The Oracle WebCenter Content: Imaging login page appears. Enter your Oracle WebLogic Server administration user name and password to log in.
Validating GridLink Data Sources for WLS_IMG2

After you finish configuring WLS_IMG1 and WLS_IMG2 and start the Administration Server and managed servers, verify that every GridLink data source you created is correctly configured and that the Oracle Notification Service (ONS) setup is correct for each data source on each managed server.

Note: These instructions assume that the host name verification displayed previously for the Oracle WSM or Oracle SOA Suite managed servers in SOAHOST2 and that the Node Manager is already running on SOAHOST2.

11.13 Configuring System MBeans for Oracle WebCenter Content: Imaging

To configure the following system MBeans for Oracle WebCenter Content: Imaging:

- InputDirectories
- SampleDirectory
- GDFontPath

1. Log in to Oracle Fusion Middleware Control at http://ADMINVHN:7001/em (Figure 11–7).
2. In the left pane, expand the farm domain name, then expand WebLogic Domain, then the domain name, then IMG_Cluster, and then click the WLS_IMG1 link.

3. At the top of the right-hand panes, click the WebLogic Server drop-down menu and choose System MBean Browser.

4. Expand Application Defined MBeans and then oracle.imaging.

5. Expand Server: WLS_IMG1 and then config.

6. Click the config bean link.

7. In the right pane, set the InputDirectories MBean to specify the path to the input files: \texttt{ORACLE\_BASE/admin/domain\_name/img\_cluster\_name/input\_files}.

   Please note that all Oracle WebCenter Content servers involved must be able to resolve this location (that is, via the NFS mount point).

8. Set the SampleDirectory MBean: \texttt{ORACLE\_BASE/admin/domain\_name/img\_cluster\_name/input\_files/Samples}.

   To process input files, the input agent must have the appropriate permissions for the input directory, and the input directory must allow file locking. The input agent requires that the user account that is running the WebLogic Server service have read and write privileges for the input directory and for all files and subdirectories in the input directory. These privileges are required so that the input agent can move the files to the various directories as it works on them. File locking on the share is needed by the input agent to coordinate actions between servers in the cluster.

9. Set the GDFontPath MBean to specify the path to the GD fonts for the X Windows environment. Check with your system administrator. The default is likely \texttt{/usr/share/X11/fonts/TTF} or \texttt{/usr/lib/X11/fonts/TTF}.

10. Click Apply.
11.14 Enabling the Imaging Feature Set in Oracle WebCenter Content

To enable the Imaging feature set in Oracle WebCenter Content:

2. Open the Administration tray or menu, and choose Admin Server.
3. On the Component Manager page, enable the IpmRepository component.
4. Click Update and confirm the action.
5. Restart the managed server, and then restart all managed servers in the Oracle WebCenter Content cluster.

11.15 Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content

To add the host names of the WLS_IMG1 and WLS_IMG2 managed servers (WCCHOST1VHN1 and WCCHOST2VHN1, respectively) to the SocketHostNameSecurityFilter parameter list:

1. Open the file ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/config/config.cfg in a text editor.
2. Remove or comment out the following line:
   
   SocketHostAddressSecurityFilter=127.0.0.1|WCCHOST1|WCCHOST2|WEBHOST1|WEBHOST2

3. Add the following two lines to include the WLS_IMG1 and WLS_IMG2 listen addresses to the list of addresses that are allowed to connect to Oracle WebCenter Content:

   SocketHostNameSecurityFilter=localhost=localhost.mycompany.com|WCCHOST1|WCCHOST2|WCCHOST1VHN1|WCCHOST2VHN1
   AlwaysReverseLookupForHost=Yes

4. Save the modified config.cfg file and restart the Oracle WebCenter Content servers for the changes to take effect.

11.16 Creating a Connection to Oracle WebCenter Content

To create a connection to Oracle WebCenter Content Server:

1. Log in to the WLS_IMG1 Imaging console at http://WCCHOST1VHN1:16000/imaging.
2. In the left-hand pane, click Manage Connections, and then Create Content Server Connection.
3. Enter a name and description for the new connection, and then click Next.
4. In the Connection Settings screen, do the following:
   - Make sure the **Use Local Content Server** checkbox is selected.
   - Set the Content Server port to 4444.
   - Add two servers to the Content Server pool:
     - WCCHOST1:4444
     - WCCHOST2:4444
   Click Next.

5. In the Connection Security screen, leave the default selections for the WebLogic user, and then click **Next**.

6. Review the connection details and click **Submit**.

### 11.17 Configuring BPEL CSF Credentials

When connecting to a BPEL system from Oracle WebCenter Content: Imaging, it is required to configure the required credential to communicate with Oracle SOA Suite. To add these credentials, use these steps:

1. On SOAHOST1, change directory to the common/bin location under the Oracle WebCenter Content home in SOAHOST1 (where your Administration Servers resides):
   ```
cd WCC_ORACLE_HOME/common/bin
   ```
   
   (*WCC_ORACLE_HOME* is the Oracle home for Oracle WebCenter Content, which is *MW_HOME*/wcc in the EDG topology.)

2. Run the Oracle WebLogic Scripting Tool (WLST):
   ```
   ./wlst.sh
   ```

3. Run `connect()` and supply the user name, password, and Administration Server URL (t3://ADMINVHN:7001).
   ```
   wls:/offline> connect()
   ```

4. Create a CSF (Credential Store Framework) credential. This credential is the credential that Imaging will use to connect to the BPEL system. It should be a BPEL admin user. CSF credentials are user name/password pairs that are keyed by an alias and stored inside a named map in the CSF. Because of its integration with OWSM web services, Oracle WebCenter Content: Imaging is currently leveraging the standard OWSM CSF map named *oracle.wsm.security*. To create a credential, use the `createCred` WLST command:
   ```
   wls:/domain_name/serverConfig> createCred(map="oracle.wsm.security", key="basic.credential", user="weblogic", password="password_for_credential")
   ```

   The key in the command is the alias, which is used for the Credential Alias property of the BPEL connection definition in the Oracle WebCenter Content: Imaging administration user interface (also the Connection.CONNECTION_BPEL_CSFKY_KEY property in the API). The alias `basic.credential` is used in the example because it is a standard default name used by OWSM and BPEL. However, the alias can be anything as long as it is unique within the map.
5. Run the list credentials command to verify that the credential was created:

```bash
wls:/domain_name/serverConfig> listCred(map="oracle.wsm.security",
key="basic.credential")
{map=oracle.wsm.security, key=basic.credential}
Already in Domain Runtime Tree

[Name : weblogic, Description : null, expiry Date : null]
PASSWORD: password_for_credential
```

11.18 Configuring a Workflow Connection

To configure a workflow connection:

1. Log in to the WLS_IMG1 imaging console at http://ECHMHOSTVHN1:16000/imaging.

2. From the navigator pane, under Manage Connections, click the Add icon and then Create Workflow Connection.

3. On the Workflow Connection Basic Information page, enter a name for the connection. The name will display in the Manage Connections panel. This field is required. Optionally, enter a brief description of the connection. The connection type defaults to Workflow Connection.

4. Click Next.

5. In the Workflow Connection Settings Page, do the following:

   a. In the HTTP Front End Address field, specify the host name or IP address, domain, and port number of the workflow server: http://soainternal.mycompany.com:80. This field is required.

   b. In the Credential Alias field, provide the credential alias created earlier as described in Section 11.17, "Configuring BPEL CSF Credentials."

   c. In the Provider field, enter your two Oracle SOA Suite server listen addresses separated by a comma: t3://SOAHOST1VHN1,SOAHOST2VHN1:8001

   d. Click the Test Connection button to confirm the connection parameters and see what composites exist on that BPEL machine.

   e. Click Next.

6. Modify the security grants if desired.

7. Click Next.

8. Click Submit.

---

**Note:** A new map will need to be created or the existing one updated if a different user and/or password is later used when integrating the Oracle SOA Suite system with a central LDAP and single sign-on (SSO) system. See Chapter 15, "Integrating with Oracle Identity Management" for details on the sample users created.
11.19 Configuring Oracle HTTP Server for the WLS_IMG Managed Servers

To enable Oracle HTTP Server to route to IMG_Cluster, which contains the WLS_IMG1 and WLS_IMG2 managed servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster as follows:

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

   ```
   # Oracle WebCenter Content: Imaging Application
   <Location /imaging>
   WebLogicCluster WCCHOST1VHN1:16000,WCCHOST2VHN1:16000
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   </Location>
   # AXF WS Invocation
   <Location /axf-ws>
   WebLogicCluster WCCHOST1VHN1:16000,WCCHOST2VHN1:16000
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   </Location>
   ```

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

   `ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohsX`

   For WEBHOST1, use `ohs1` for `ias-component` and for WEBHOST2 use `ohs2`.

11.20 Setting the Frontend HTTP Host and Port

You must set the frontend HTTP host and port for the Oracle WebLogic Server Imaging cluster (IMG_Cluster):

1. Log in to WebLogic Server Administration Console.
2. Go to the Change Center section and click Lock & Edit.
3. Expand the Environment node in the Domain Structure window.
4. Click Clusters.
5. On the Summary of Clusters page, select IMG_Cluster.
6. Open the HTTP tab.
7. Set the following values:
   - Frontend Host: wcc.mycompany.com
   - Frontend HTTPS Port: 443
   - Frontend HTTP Port: 80
8. Click Save.
9. Click Activate Changes in the Change Center section of the Administration Console.
10. Restart the servers to make the frontend host directive in the cluster take effect.
11.21 Validating Access Through Oracle HTTP Server

Verify URLs to ensure that appropriate routing and failover is working from the HTTP Server to the IMG_Cluster. To verify the URLs:

1. While WLS_IMG2 is running, stop WLS_IMG1 using the WebLogic Server Administration Console.
2. Access http://WEBHOST1:7777/imaging to verify it is functioning properly. (Please note that you will not be able to retrieve reports or data since the Imaging server is down.)
3. Start WLS_IMG1 from the WebLogic Server Administration Console.
4. Stop WLS_IMG2 from the WebLogic Server Administration Console.
5. Access http://WEBHOST1:7777/imaging to verify it is functioning properly.
6. Start WLS_IMG2 from the WebLogic Server Administration Console.

11.22 Configuring Node Manager for the WLS_IMG Managed Servers

It is assumed that the host names used by the WLS_IMG managed servers as listen addresses have already been configured for host name verification as explained in Section 10.15, "Configuring Node Manager for the WLS_WCC and WLS_IMG Managed Servers."

At this point, once the Imaging managed servers have been added to the domain, the procedure in Section 13.3.5, "Configuring Managed Servers to Use the Custom Keystores" should be performed so that the servers are configured to use custom key stores.

11.23 Configuring Server Migration for the WLS_IMG Managed Servers

Server migration is required for proper failover of the Oracle WebCenter Content: Imaging components in the event of failure in any of the WCCHOST1 and WCCHOST2 nodes. See Chapter 14, "Configuring Server Migration for an Enterprise Deployment" for further details. For Oracle WebCenter Content: Imaging, use the following values for the variables in that chapter:

- Server names:
  - WLS_SERVER1: WLS_IMG1
  - WLS_SERVER2: WLS_IMG2
- Host names:
  - HOST1: WCCHOST1
  - HOST2: WCCHOST2
- Cluster name:
  - CLUSTER: IMG_Cluster
11.24 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. This backup can be discarded 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 for information on database backup.

To back up the installation at this point:
1. Back up the web tier on WEBHOST1:
   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 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 and managed 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 in SOAHOST1 to create the backup:
   ```
   tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
   ```
This chapter describes how to extend a domain with Oracle WebCenter Content: Inbound Refinery using the Oracle Fusion Middleware Configuration Wizard. It contains the following sections:

- Section 12.1, "Overview of Extending the Domain for Oracle WebCenter Content: Inbound Refinery"
- Section 12.2, "Associating Inbound Refinery Managed Servers with Virtual Host Names"
- Section 12.3, "Extending the Domain to Include Inbound Refinery"
- Section 12.4, "Starting Node Manager on WCCHOST1 and WCCHOST2"
- Section 12.5, "Propagating the Domain Configuration to the Managed Server Domain Directories"
- Section 12.6, "Restarting the Administration Server"
- Section 12.7, "Starting the Inbound Refinery Managed Servers"
- Section 12.8, "Configuring the Inbound Refineries"
- Section 12.9, "Validating the Configuration of the Inbound Refinery Managed Servers"

Note: Before starting the setup process, read the release notes for additional installation and deployment information. They are available on the Oracle Fusion Middleware Documentation Library at http://docs.oracle.com/cd/E23943_01/relnotes.htm.

12.1 Overview of Extending the Domain for Oracle WebCenter Content: Inbound Refinery

Oracle WebCenter Content: Inbound Refinery is required for document conversion by Oracle WebCenter Content Server. The actual number of Inbound Refinery managed servers varies depending on requirements. For availability reasons, Oracle recommends configuring at least two Inbound Refinery managed servers. Configure these servers on separate machines. In the reference Oracle WebCenter Content enterprise deployment topology, Inbound Refinery will be configured on the same machine as Content Server.
Even though a cluster is created in the process of extending the domain with Inbound Refinery, each Inbound Refinery instance is completely independent. Clustering is used for management purposes only.

Extend the domain to include Oracle WebCenter Content: Inbound Refinery. Table 12–1 lists the steps for configuring WebCenter Content and other tasks required for extending the domain with Inbound Refinery managed servers.

Table 12–1  Steps for Extending the Domain with Inbound Refinery

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for extending the domain for Inbound Refinery</td>
<td>Associating WLS_IBR1 and WLS_IBR2 with virtual host names.</td>
<td>Section 12.2, “Associating Inbound Refinery Managed Servers with Virtual Host Names”</td>
</tr>
<tr>
<td>Extend the domain for Inbound Refinery</td>
<td>Extend the WebLogic domain you created in Chapter 8, “Creating a Domain for an Enterprise Deployment.”</td>
<td>Section 12.3, “Extending the Domain to Include Inbound Refinery”</td>
</tr>
<tr>
<td>Start Node Manager</td>
<td>Run the setNMProps.sh script and then start Node Manager on WCCHOST1 and on WCCHOST2.</td>
<td>Section 12.4, “Starting Node Manager on WCCHOST1 and WCCHOST2”</td>
</tr>
<tr>
<td>Propagate the domain configuration to the Inbound Refinery managed servers</td>
<td>Propagate the start scripts and classpath configuration from the Administration Server’s domain directory to the managed server domain directories.</td>
<td>Section 12.5, “Propagating the Domain Configuration to the Managed Server Domain Directories”</td>
</tr>
<tr>
<td>Restart the Administration Server for the domain</td>
<td>Stop and then start the Administration Server to make the changes from the previous step take effect.</td>
<td>Section 12.6, “Restarting the Administration Server”</td>
</tr>
<tr>
<td>Start the Inbound Refinery managed servers</td>
<td>Start the WLS_IBR1 and WLS_IBR2 managed servers.</td>
<td>Section 12.7, “Starting the Inbound Refinery Managed Servers”</td>
</tr>
<tr>
<td>Configure the Inbound Refinery instances</td>
<td>Complete the initial configuration of Inbound Refinery on WLS_IBR1 and WLS_IBR</td>
<td>Section 12.8, “Configuring the Inbound Refineries”</td>
</tr>
<tr>
<td>Verify the Inbound Refinery configuration</td>
<td>Verify that a file with an extension recognized as valid for conversion is correctly converted on Content Server.</td>
<td>Section 12.9, “Validating the Configuration of the Inbound Refinery Managed Servers”</td>
</tr>
</tbody>
</table>

12.2 Associating Inbound Refinery Managed Servers with Virtual Host Names

Associate the WLS_IBR1 and WLS_IBR2 servers with the virtual host names WCCHOST1VHN1 and WCCHOST2VHN1. Check that these virtual host names are enabled by DNS or /etc/hosts resolution in your system and that they map to the appropriate VIPs.

For more information, see Section 9.2, "Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2."
12.3 Extending the Domain to Include Inbound Refinery

To complete the enterprise deployment topology, 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 created the repository schema is running. For Oracle RAC databases, it is recommended that all instances are running, so that the validation check later on becomes more reliable.

2. On SOAHOST1, 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 the node where the Administration Server resides).

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

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

4. In the Welcome screen, select **Extend an existing WebLogic domain**, and click Next.

5. In the WebLogic Domain Directory screen, select the WebLogic domain directory (ORACLE_BASE/admin/domain_name/aserver/domain_name), and click Next.

6. 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]**

     This is the selection for Oracle WebCenter Content: Inbound Refinery.

The following products should already be selected and grayed out. They were selected when you created a domain in Section 8.3, "Running the Configuration Wizard on SOAHOST1 to Create a Domain," or extended the domain in Section 9.3, "Extending the Domain for Oracle SOA Suite Components Using the Configuration Wizard," Section 10.3, "Extending the Domain to Include WebCenter Content," or Section 11.3, "Extending the Domain to Include Imaging":

- **Basic WebLogic Server Domain**
- **Oracle SOA Suite for developers**
- **Oracle SOA Suite**
- **Oracle WebCenter Content: Imaging**
- **Oracle Universal Content Management - Content Server**
- **Oracle Enterprise Manager**
- Oracle WSM Policy Manager
- Oracle JRF

Click Next.

7. In the Configure GridLink RAC Component Schema screen, nothing needs to be done. Inbound Refinery does not have a schema in the database. Click Next to continue.

8. In the Test JDBC Component Schema screen, nothing needs to be done. Click Next to continue.

9. In the Optional Configuration screen, select the following options:
- Managed Servers, Clusters and Machines
- Deployment and Services

Click Next.

10. In the Configure Managed Servers screen, add a managed server for Inbound Refinery and configure the Inbound Refinery servers.

One server is created automatically. Rename this server to WLS_IBR1, and add a new server named WLS_IBR2. Give these servers the attributes listed in Table 12-2. Do not modify the other servers that are shown in this screen; leave them as they are.
11. In the Configure Clusters screen, click **Add** to add the Inbound Refinery cluster shown in Table 12–3. Do not modify the other clusters that appear in this screen; leave them as they are.

12. In the Assign Servers to Clusters screen (Figure 12–2), add the following items:
   - **IBR_Cluster**:
     - WLS_IBR1
     - WLS_IBR2
Do not modify the other assignments that appear in this screen; leave them as they are.

Click Next.

13. In the Configure Machines screen, click Next.

14. In the Assign Servers to Machines screen (Figure 12–3), assign the Inbound Refinery managed servers to machines as follows:
   - Assign WLS_IBR1 to WCCHOST1.
   - Assign WLS_IBR2 to WCCHOST2.
Extending the Domain to Include Inbound Refinery

Figure 12–3 Assign Inbound Refinery Servers to Machines

Click Next.

15. In the Target Deployments to Clusters or Servers screen, verify the following targets:
   - The usermessagingserver and usermessagingdriver-email deployments 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.*, and oracle.soa.* deployments should be targeted only to SOA_Cluster, except for the oracle.soa.workflow.wc library, which should be targeted to both SOA_Cluster and IMG_Cluster.

Click Next.

16. In the Target Services to Clusters or Servers screen, click Next.

17. In the Configuration Summary screen, click Extend.

18. In the Creating Domain screen, click Done.

19. Restart the Administration Server to make these changes take effect.

For more information, see Section 12.6, "Restarting the Administration Server."
12.4 Starting Node Manager on WCCHOST1 and WCCHOST2

To start Node Manager on WCCHOST1 and WCCHOST2 if Node Manager has not started already:

1. On both WEBHOST1 and WEBHOST2, 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. See also Section 16.11.3, "Incomplete Policy Migration After Failed Restart of SOA Server."

   **Note:** If the Inbound Refinery server is sharing the MW_HOME in a local or shared storage with Oracle WebCenter Content, 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 and it is likely already running in the node for Oracle WebCenter Content.

2. Run the following commands on both WCCHOST1 and WCCHOST2 to start Node Manager:

   cd WL_HOME/server/bin
   ./startNodeManager.sh

12.5 Propagating the Domain Configuration to the Managed Server Domain Directories

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 WCCHOST2:

   **Note:** Assuming that WCCHOST1 shares the ORACLE_HOME with SOAHOST1, the template will be present in the same directory in WCCHOST1; otherwise, copy it also to WCCHOST1.

   scp edgdomaintemplateIBR.jar oracle@WCCHOST2:ORACLE_BASE/product/fmw/oracle_common/common/bin
3. Run the `unpack` command on WCCHOST1 to unpack the propagated template.

```bash
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template=edgdomaintemplateIBR.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications -overwrite_domain=true
```

**Note:** Make sure to run `unpack` from the `ORACLE_COMMON_HOME/common/bin` directory, not from `WL_HOME/common/bin`.

4. Repeat step 3 for WCCHOST2.

### 12.6 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 8.4.4, "Starting the Administration Server on SOAHOST1."

### 12.7 Starting the Inbound Refinery Managed Servers

To start the WLS_IBR1 managed server on WCCHOST1:

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 from the Servers column of the table.
5. Click Start.

Repeat these steps to start the WLS_IBR2 managed server on WCCHOST2.

### 12.8 Configuring the Inbound Refineries

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 Refinery instances. The process for configuring Oracle WebCenter Content is to add each Inbound Refinery instance as a provider. There are also post-installation steps that must be performed with Inbound Refinery.

The following sections describe the procedures for post-installation configuration of each Inbound Refinery instance:

- Section 12.8.1, "Configuring Inbound Refinery Settings"
- Section 12.8.2, "Configuring Document Conversion"
- Section 12.8.3, "Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion"

### 12.8.1 Configuring Inbound Refinery Settings

To configure the settings for each Inbound Refinery instance:

1. Access the Inbound Refinery post-installation configuration screen at the following URL, in which \( N \) is 1 or 2:
   
   [\text{http://WCCHOST}\_N:16250/ibr/]

2. In the Configuration screen, you will see Inbound Refinery Instance Identifier: \( \text{name} \). Set the configuration settings for this instance as follows:

   - **Inbound Refinery Instance Folder:** Set this to \( \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain_name/ibr_cluster_name/ibr}\_N \). 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 \( \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain_name/ibr_cluster_name/ibr}\_N/vault \).
   - **WebLayout Folder:** Set this to \( \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain_name/ibr_cluster_name/ibr}\_N/weblayout \).
   - **User Profile Folders:** Set this to \( \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain_name/ibr_cluster_name/ibr}\_N/data/users/profiles \).
   - **Incoming Socket Connection Address Security Filter:** Set this to a pipe-delimited list of localhost and the server IPs:
     
     127.0.0.1|\text{WCCHOST1-IP}|\text{WCCHOST2-IP}|\text{WEBHOST1-IP}|\text{WEBHOST2-IP}

   This enables access from Oracle WebCenter Content Server. The values for \( \text{WCCHOST1-IP} \) and \( \text{WCCHOST2-IP} \) 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 \( \text{SocketHostAddressSecurityFilter} \) in \( \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain_name/mserver/domain_name/ucm/ibr/config/config.cfg} \) 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/msserver/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.

Click **Submit**, and you should get the following message:

Post-install configuration complete. Please restart this node.

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*.

### 12.8.2 Configuring Document Conversion

To configure document conversion on each Inbound Refinery managed server:

1. Log in to Inbound Refinery at the following URL, in which \( N \) is 1 or 2

   \[ \text{http://WCCHOST:16250/ibr/} \]

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:

   a. Open the **Administration** tray or menu, then choose **Admin Server**.

   b. In the Component Manager, select **PDFExportConverter** in Inbound Refinery and any other components you want. 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. 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. Restart the Administration Server and all Inbound Refinery managed servers.

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.

12.8.3 Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion

Before Oracle WebCenter Content Server can send jobs to Inbound Refinery for conversion, you need to perform these setup tasks for each Inbound Refinery managed server:

- Creating an Outgoing Provider
- Enabling Components for Inbound Refinery on Content Server
- Selecting File Formats To Be Converted

12.8.3.1 Creating an Outgoing Provider

Before Content Server can send files to Inbound Refinery for conversion, you must set up an outgoing provider from Content Server to each Inbound Refinery with the Handles Inbound Refinery Conversion Jobs option checked.

Perform these tasks to create an outgoing provider for each Inbound Refinery:

1. Log in to Oracle WebCenter Content Server at the following URL:
   http://WCCHOST1:16200/cs/

2. Open the Administration tray or menu and choose Providers.

3. In the Create a New Provider section of the Providers page, click Add in the outgoing row.

4. Enter the following values for the fields:
   - Provider Name: Any short name with no spaces. It is a good idea to use the same value as the Instance Name value
   - 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.

Note: For information about the conversion components, see "Inbound Refinery Conversion Options and Related Components" in Oracle WebCenter Content Administrator’s Guide for Conversion.
**Server Port:** The value of the Server Socket Port field for the Inbound Refinery instance as specified in Section 12.8.1, "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 12.8.1, "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/.

5. Under Conversion Options, check Handles Inbound Refinery Conversion Jobs. Do not check Inbound Refinery Read Only Mode.

6. Click Add.

7. Restart Oracle WebCenter Content Server.

8. Go back to the Providers page, and check that the Connection State value is good for the provider.
   
   If the value is not good, double-check that you entered all the preceding entries correctly, and check that the Content Server and Inbound Refinery instances can ping each other.

For more information about setting up providers, see “Configuring Content Server and Refinery Communication” in Oracle WebCenter Content Administrator’s Guide for Conversion.

**12.8.3.2 Enabling Components for Inbound Refinery on Content Server**

Some conversion types require helper components to be enabled on Content Server. The InboundRefinerySupport component must always be enabled on any Content Server instance that uses Inbound Refinery for document conversion. It is enabled by default on a new Content Server installation.

To enable Inbound Refinery components on Content Server:

1. Log in to Oracle WebCenter Content Server at the following URL:
   
   http://WCCHOST1:16200/cs/

2. Open the Administration tray or menu, then choose Admin Server, and then Component Manager.

3. Under Inbound Refinery, make sure InboundRefinerySupport is selected, and select any other components, such as XMLConverterSupport, that you want to enable.

4. Click Update.

5. Restart Oracle WebCenter Content Server.

**12.8.3.3 Selecting File Formats To Be Converted**

To tell Oracle WebCenter Content Server which files to send to Inbound Refinery to be converted, you need to select file formats.
To select file formats to be converted:

1. Log in to Oracle WebCenter Content Server at the following URL:
   http://WCHOST1:16200/cs/

2. Open the Administration tray or menu, then choose Refinery Administration,
   and then File Formats Wizard to open the File Formats Wizard page, which
   specifies what file formats will be sent to Inbound Refinery for conversion when
   they are checked into Content Server.

3. Select the formats you want converted, such as doc, dot, docx, and dotx for
   Microsoft Word documents.

4. Click Update.

You can also select file formats with the Configuration Manager, with more
fine-grained control, including file formats that wizard does not list. For more
information, see "Using the File Formats Wizard" and "Using the Configuration
Manager" in Oracle WebCenter Content Administrator’s Guide for Conversion.

**12.9 Validating the Configuration of the Inbound Refinery Managed Servers**

To ensure that the Inbound Refinery managed servers you have created are properly
configured, validate the configuration by logging in to Oracle WebCenter Content
Server and verifying that a file with an extension recognized as valid for conversion is
correctly converted.

For example, if you selected docx as a format to be converted, you can convert a
Microsoft Word document with a .docx extension to PDF format.
This chapter describes how to configure Node Manager in accordance with the EDG recommendations. It contains the following sections:

- Section 13.1, "Overview of Setting Up Node Manager"
- Section 13.2, "Changing the Location of the Node Manager Log"
- Section 13.3, "Enabling Host Name Verification Certificates for Node Manager"
- Section 13.4, "Starting Node Manager"

### 13.1 Overview of Setting Up Node Manager

Node Manager enables you to start and stop the Administration Server and the managed servers for an Oracle WebLogic Server domain. Table 13–1 describes the setup steps, followed by an overview of the setup process and Oracle recommendations for the location of the Node Manager log and host name verification.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a location for the Node Manager log within the admin directory for the ED.</td>
<td>Edit the LogFile property in the nodemanager.properties file, and restart Node Manager.</td>
<td>Section 13.2, &quot;Changing the Location of the Node Manager Log&quot;</td>
</tr>
<tr>
<td>Set up SSL communication between Node Manager and the Administration Server</td>
<td>Generate self-signed certificates, create trust and identity keystores, configure Node Manager and the managed servers to use the custom keystores, and change the host name verification setting for each managed server.</td>
<td>Section 13.3, &quot;Enabling Host Name Verification Certificates for Node Manager&quot;</td>
</tr>
<tr>
<td>Start Node Manager</td>
<td>Run the setNMProps.sh script before starting Node Manager the first time.</td>
<td>Section 13.4, &quot;Starting Node Manager&quot;</td>
</tr>
</tbody>
</table>

### Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topology outlined in Section 2.1.1, "Reference Topology Documented in the Guide." Variables are used in this chapter to distinguish between component-specific items:

- **WLS_SERVER**: this refers to a managed WebLogic server for the enterprise deployment component (for example, WLS_SOA1).
Changing the Location of the Node Manager Log

- **HOST**: this refers to a host machine for the enterprise deployment component (for example, SOAHOST1).
- **VIP**: this refers to a virtual IP for the enterprise deployment component (for example, SOAHOST1VHN1).

The values to be used to these variables are provided in the component-specific chapters in this EDG. Please note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

**Recommendations**

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware Home where Node Manager resides). See Section 13.2, “Changing the Location of the Node Manager Log” for further details.

2. Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See Section 13.3, ”Enabling Host Name Verification Certificates for Node Manager” for further details.

---

**Note**: The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

### 13.2 Changing the Location of the Node Manager Log

Edit the Node Manager properties file located at `MW_HOME/wlserver_10.3/common/nodemanager/nodemanager.properties`. Add the new location for the log file, using the following line:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Oracle recommends that this location is outside the `MW_HOME` directory and inside the admin directory for the EDG.

Restart Node Manager for the change to take effect.

### 13.3 Enabling Host Name Verification Certificates for Node Manager

Setting up SSL for communication between Node Manager and the Administration Server consists of the following steps:

- **Step 1**: Generating Self-Signed Certificates Using the `utils.CertGen` Utility
- **Step 2**: Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility
- **Step 3**: Creating a Trust Keystore Using the Keytool Utility
- **Step 4**: Configuring Node Manager to Use the Custom Keystores
Enabling Host Name Verification Certificates for Node Manager

- Step 5: Configuring Managed Servers to Use the Custom Keystores
- Step 6: Changing the Host Name Verification Setting for the Managed Servers

13.3.1 Generating Self-Signed Certificates Using the \texttt{utils.CertGen} Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (\texttt{HOST.mycompany.com}) and a WLS managed server listens on a virtual host name (\texttt{VIP.mycompany.com}). Whenever a server is using a virtual host name, it is implied that the server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example will need to be extended to:

1. Add the required host names to the certificate stores (if they are different from \texttt{HOST.mycompany.com} and \texttt{VIP.mycompany.com}).

2. Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by managed servers).

Follow the steps below to create self-signed certificates on \texttt{HOST}. These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in \textit{Oracle Fusion Middleware Securing Oracle WebLogic Server}. The examples below configure certificates for \texttt{HOST.mycompany.com} and \texttt{VIP.mycompany.com}; that is, it is assumed that both a physical host name (\texttt{HOST}) and a virtual host name (\texttt{VIP}) are used in \texttt{HOST}. It is also assumed that \texttt{HOST.mycompany.com} is the address used by Node Manager and \texttt{VIP.mycompany.com} is the address used by a managed server or the Administration Server. This is the common situation for nodes hosting an Administration Server and a Fusion Middleware component, or for nodes where two managed servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the \texttt{WL_HOME/server/bin/setWLSEnv.sh} script. In the Bourne shell, run the following commands on \texttt{HOST}:

   ```
   cd \texttt{WL_HOME/server/bin}
   . ./setWLSEnv.sh
   ```

   Verify that the \texttt{CLASSPATH} environment variable is set:

   ```
   echo \$CLASSPATH
   ```

2. The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, and so on). In this case, SOAHOST2 uses the cert directory created for SOAHOST1 certificates. Create a user-defined directory for the certificates:

   ```
   mkdir cert
   ```

3. Change directory to the directory that you just created:

   ```
   cd cert
   ```
4. Run the `utils.CertGen` tool from the user-defined directory on `HOST` to create the certificates for both `HOST`, mycompany.com and `VIP`, mycompany.com.

Syntax (all on a single line):

```
java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
[export | domestic] [Host_Name]
```

Examples:

```
java utils.CertGen welcome1 HOST.mycompany.com_cert HOST.mycompany.com_key
domestic HOST.mycompany.com

java utils.CertGen welcome1 VIP.mycompany.com_cert VIP.mycompany.com_key
domestic VIP.mycompany.com
```

### 13.3.2 Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility

Follow these steps to create an identity keystore on `HOST`:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, `ORACLE_BASE/admin/domain_name/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. On `HOST`, import the certificate and private key for both `HOST.mycompany.com` and `VIP.mycompany.com` into the identity store. Make sure that you use a different alias for each of the certificate/key pairs imported.

Syntax (all on a single line):

```
java utils.ImportPrivateKey Keystore_File Keystore_Password
Certificate_Alias_to_Use Private_Key_Passphrase
Certificate_File Private_Key_File
[Keystore_Type]
```

Examples:

```
java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity1 welcome1
ORACLE_BASE/admin/domain_name/cert/HOST.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/HOST.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity2 welcome1
ORACLE_BASE/admin/domain_name/cert/VIP.mycompany.com_cert.pem
ORACLE_BASE/admin/domain_name/cert/VIP.mycompany.com_key.pem
```

### 13.3.3 Creating a Trust Keystore Using the `Keytool` Utility

Follow these steps to create the trust keystore on `HOST`:

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java
keystore CA certificates on HOST 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/cert/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 -storepass -new New_Password -keystore Trust_Keystore -storepass Original_Password
```

For example:

```
keytool -storepass -new welcome1 -keystore appTrustKeyStore.jks -storepass changeit
```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the WL_HOME/server/lib directory. This CA certificate must be imported into the appTrustKeyStore using the keytool utility on HOST. The syntax is:

```
keytool -import -v -noprompt -trustcacerts -alias Alias_Name -file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_HOME/server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass welcome1
```

### 13.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the nodemanager.properties file located in the WL_HOME/common/nodemanager directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

Make sure to use the correct value for CustomIdentityAlias on each node; that is, the custom identity alias specifically assigned to that node, for example for ...HOST2:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/cert/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity2
CustomIdentityPrivateKeyPassPhrase=welcome1
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager as described in Section 13.4, "Starting Node Manager." For security reasons, you want to minimize the time the entries in the nodemanager.properties file are left unencrypted. After you edit the file, you should start Node Manager as soon as possible so that the entries get encrypted.

When using a common/shared storage installation for MW_HOME, Node Manager is started from different nodes using the same base configuration.
Enabling Host Name Verification Certificates for Node Manager

(nodemanager.properties). In that case, it is required to add the certificate for all the nodes that share the binaries to the appIdentityKeyStore.jks identity store. To do this, create the certificate for the new node and import it to appIdentityKeyStore.jks as in Section 13.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility." Once the certificates are available in the store, each node manager needs to point to a different identity alias to send the correct certificate to the Administration Server. To do this, set different environment variables on HOST before starting Node Manager in the different nodes:

cd WL_HOME/server/bin

export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX

---

Note: Make sure to specify the custom identity alias specifically assigned to each host, so appIdentity1 for ...HOST1 and appIdentity2 for ...HOST2.

---

13.3.5 Configuring Managed Servers to Use the Custom Keystores

Follow these steps to configure the identity and trust keystores for WLS_SERVER:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click Lock & Edit.
3. Expand the Environment node in the Domain Structure window.
4. Click Servers.
5. On the Summary of Server page, click the name of the server for which you want to configure the identity and trust keystores (WLS_SERVER).
6. On the settings page for the selected server, select Configuration and then Keystores.
7. Click the Change button next to the Keystores field and select the Custom Identity and Custom Trust method for storing and managing private keys/digital certificate pairs and trusted CA certificates. Click Save when you are done.
8. In the Identity section, define attributes for the identity keystore:
   - Custom Identity Keystore: The fully qualified path to the identity keystore:
     
     ORACLE_BASE/admin/domain_name/cert/appIdentityKeyStore.jks
   - Custom Identity Keystore Type: Leave blank; it defaults to JKS.
   - Custom Identity Keystore Passphrase: The password (Keystore_Password) you provided in Section 13.3.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether or not you define this property depends on the requirements of the keystore.
9. In the Trust section, define properties for the trust keystore:
   - Custom Trust Keystore: The fully qualified path to the trust keystore:
     
     ORACLE_BASE/admin/domain_name/cert/appTrustKeyStore.jks
   - Custom Trust Keystore Type: Leave blank; it defaults to JKS.
■ Custom Trust Keystore Passphrase: The password you provided as New Password in Section 13.3.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether or not you define this property depends on the requirements of the keystore.

10. Click Save.
11. Click Activate Changes in the Administration Console’s Change Center to make the changes take effect.
12. Select Configuration, then SSL.
13. Click Lock & Edit.
14. In the Private Key Alias field, enter the alias you used for the host name the managed server listens on.

In the Private Key Passphrase and the Confirm Private Key Passphrase fields, enter the password for the keystore that you created in Section 13.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."

15. Click Save.
16. Click Activate Changes in the Administration Console’s Change Center to make the changes take effect.
17. Restart the server for which the changes have been applied.

13.3.6 Changing the Host Name Verification Setting for the Managed Servers

Once the steps above have been performed, you should set host name verification for the affected managed servers to Bea Host Name Verifier. To do this, perform the following steps:

1. Log in to WebLogic Server Administration Console.
2. Expand the Environment node in the Domain Structure window.
3. Click Servers.
4. On the Summary of Servers page, select the managed server in the Names column of the table.
5. On the settings page for the server, open the SSL tab.
6. Expand the Advanced section of the page.
7. Click Lock & Edit.
8. Set host name verification to Bea Host Name Verifier.
9. Click Save.
10. Restart the server for which the changes have been applied.

13.4 Starting Node Manager

Run the commands below to start Node Manager on HOST. If you have not configured and started Node Manager for the first time yet, run the setNMProps.sh script as specified in Section 8.4.3, "Starting Node Manager on SOAHOST1" to enable the use of the start script for your managed servers.
Starting Node Manager

---

**Note:** Make sure to specify the custom identity alias specifically assigned to each host, so `appIdentity1` for `...HOST1` and `appIdentity2` for `...HOST2`.

```bash
cd $WL_HOME/server/bin
export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX
./startNodeManager.sh
```
14

Configuring Server Migration for an Enterprise Deployment

This chapter describes the procedures for configuring server migration for an 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 GridLink Data Source for Leasing Using the Administration Console"
- Section 14.4, "Enabling Host Name Verification Certificates between HOST1 and HOST2 and the Administration Server"
- Section 14.5, "Editing 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 the Server Migration"

14.1 Overview of Server Migration for an Enterprise Deployment

You can configure server migration for Oracle WebLogic Server managed servers. With server migration configured, should failure occur, each managed server can restart on a different host machine. The managed servers listen on specific floating IPs that are failed over by Oracle WebLogic Server.

Note: Refer to each component’s chapter for details on whether it uses or requires server migration or not.

The procedures described in this chapter must be performed for various components of the enterprise deployment topology outlined in Section 2.1.1, "Reference Topology Documented in the Guide." Variables are used in this chapter to distinguish between component-specific items:

- WLS_SERVER1 and WLS_SERVER2 refer to the Oracle WebLogic Server managed servers for the enterprise deployment component.
HOST1 and HOST2 refer to the host machines for the enterprise deployment component.

CLUSTER refers to the cluster associated with the enterprise deployment component.

The values to be used for these variables are provided in the component-specific chapters in this EDG.

In this enterprise topology, you must configure server migration for the WLS_SERVER1 and WLS_SERVER2 managed servers. The WLS_SERVER1 managed server is configured to restart on HOST2 should a failure occur. The WLS_SERVER2 managed server is configured to restart on HOST1 should a failure occur. For this configuration, the WLS_SERVER1 and WLS_SERVER2 servers listen on specific floating IP addresses that are failed over by Oracle WebLogic Server migration.

Table 14–1 describes the steps for configuring server migration for the Oracle WebLogic Server managed servers.

Table 14–1  Steps for Configuring Server Migration

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up a user, tablespace, and migration table</td>
<td>Create a Leasing tablespace, user, and table for server migration.</td>
<td>Section 14.2, &quot;Setting Up a User and Tablespace for the Server Migration Leasing Table&quot;</td>
</tr>
<tr>
<td>Create GridLink data sources for the Leasing table</td>
<td>Create a data source for each of the Oracle RAC database instances and the global Leasing GridLink data source in the Administration Console.</td>
<td>Section 14.3, &quot;Creating a GridLink Data Source for Leasing Using the Administration Console&quot;</td>
</tr>
<tr>
<td>Specify Node Manager properties values for migration</td>
<td>Edit the property values in the nodemanager.properties file for each host, and verify the values.</td>
<td>Section 14.5, &quot;Editing Node Manager’s Properties File&quot;</td>
</tr>
<tr>
<td>Set the environment and specify superuser privileges for the oracle user</td>
<td>Add files to the PATH environment variable, and grant sudo configuration for the wlsifconfig.sh script.</td>
<td>Section 14.6, &quot;Setting Environment and Superuser Privileges for the wlsifconfig.sh Script&quot;</td>
</tr>
<tr>
<td>Configure cluster migration</td>
<td>Assign available nodes as migration targets, and specify candidate machines for each server.</td>
<td>Section 14.7, &quot;Configuring Server Migration Targets&quot;</td>
</tr>
<tr>
<td>Test server migration</td>
<td>Verify server migration between hosts from Node Manager or the Administration Console.</td>
<td>Section 14.8, &quot;Testing the Server Migration&quot;</td>
</tr>
</tbody>
</table>

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.

**Note:** If other servers in the same domain have already been configured for server migration, you can use the same tablespace and data sources. In that case, the data sources and GridLink data source for the database Leasing do not need to be re-created, but they will have to be retargeted to the cluster being configured with server migration.
To set up a user and tablespace for the server migration Leasing table:

1. Create a tablespace called Leasing. For example, log in 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;

   **Note:** The database file location will vary depending on the type of storage and data file location used for the database.

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 GridLink Data Source for Leasing Using the Administration Console

Create a GridLink data source for the Leasing table from the WebLogic Server Administration Console.

To create a GridLink data source:

1. Log in to the WebLogic Server Administration Console.

2. If you have not already done so, in the Change Center, click Lock & Edit and click Next.

3. In the Domain Structure tree, expand Services, then select Data Sources.

4. On the Summary of Data Sources page, click New and select GridLink Data Source, and enter the following:

   - Enter a logical name for the data source in the Name field. For example, Leasing.
   - Enter a name for JNDI. For example, jdbc/leasing.
For the Database Driver, select Oracle's Driver (Thin) for GridLink Connections Versions 11 and later.

Click Next.

5. In the Transaction Options page, de-select Supports Global Transactions, and click Next.

6. In the GridLink Data Source Connection Properties Options screen, select Enter individual listener information and click Next.

7. Enter the following connection properties:

- **Service Name**: Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example:
  
  wccedg.mycompany.com

- **Host Name and Port**: Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the appropriate parameter in the database using the TCP Protocol:

  SQL> show parameter remote_listener;

  NAME                 TYPE        VALUE
  --------------------------------------------------
  remote_listener     string      db-scan.mycompany.com

  **Note**: For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener; for example:

  custdbhost1-vip.mycompany.com (port 1521)

  and

  custdbhost2-vip.mycompany.com (1521)

  For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database. For information about configuring multi data sources, see Appendix A, "Using Multi Data Sources with Oracle RAC."

- **Port**: The port on which the database server listens for connection requests.

- **Database User Name**: Leasing

- **Password**: For example: welcome1

- **Confirm Password**: Enter the password again and click Next.

8. On the Test GridLink Database Connection page, review the connection parameters and click Test All Listeners. Here is an example of a successful connection notification:

  Connection test for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_ LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=db-scan.mycompany.com) (PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=wccedg.example.com))) succeeded.

  Click Next.
9. In the ONS Client Configuration page, do the following:
   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.
   - Enter here also the SCAN address for the RAC database and the ONS remote port as reported by the database (example follows) and click **ADD**:
     
     ```
     [orcl@db-scan1 ~]$ srvctl config nodeapps -s
     ONS exists: Local port 6100, remote port 6200, EM port 2016
     ```
   - Click **Next**.

   **Note:** For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service; for example:

   custdbhost1.mycompany.com (port 6200)

   and

   custdbhost2.mycompany.com (6200)

10. On the Test ONS Client Configuration page, review the connection parameters, and click **Test All ONS Nodes**.
    
    Here is an example of a successful connection notification:

    Connection test for db-scan.mycompany.com:6200 succeeded.

    Click **Next**.

11. In the Select Targets page, select **WCC_Cluster** as the target, and **All Servers in the cluster**.

12. Click **Finish**.

13. Click **Activate Changes**.

### 14.4 Enabling Host Name Verification Certificates between HOST1 and HOST2 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 13.3, "Enabling Host Name Verification Certificates for Node Manager."**
14.5 Editing Node Manager's Properties File

The third step is to edit Node Manager's properties file. This needs to be done for the Node Managers in both nodes where server migration is being configured:

```
Interface=eth0
NetMask=255.255.255.0
UseMACBroadcast=true
```

- **Interface**: This property specifies the interface name for the floating IP (for example, eth0).
  
  Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. 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, eth2, eth3, ethn, depending on the number of interfaces configured.

- **NetMask**: This property specifies the net mask for the interface for the floating IP. The net mask should be the same as the net mask on the interface; 255.255.255.0 is used as an example in this document.

- **UseMACBroadcast**: 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 Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
...  
StateCheckInterval=500  
Interface=eth0  
NetMask=255.255.255.0  
...  
```

**Note**: The steps below are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. Set the following property in the nodemanager.properties file:

   - **StartScriptEnabled**: Set this property to true. This is required for Node Manager to start the managed servers using start scripts.

2. Start Node Manager on HOST1 and HOST2 by running the `startNodeManager.sh` script, which is located in the `WL_HOME/server/bin` directory.

**Note**: When you run 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 HOSTn, use the Interface environment variable as follows:

```
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

The fourth step is to set environment and superuser privileges for the wlsifconfig.sh script (for the oracle user):

1. Ensure that your PATH environment variable includes the files listed in Table 14–2.

<table>
<thead>
<tr>
<th>File</th>
<th>Located in this directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlsifconfig.sh</td>
<td>ORACLE_BASE/admin/domain_name/mserver/domain_name/bin/server_migration</td>
</tr>
<tr>
<td>wlscontrol.sh</td>
<td>WL_HOME/common/bin</td>
</tr>
<tr>
<td>nodemanager.domains</td>
<td>WL_HOME/common/nodemanager</td>
</tr>
</tbody>
</table>

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, perform these steps 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 over ifconfig and arping:

   ```bash
   oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
   ```

   **Note:** Ask the system administrator for the sudo and system rights as appropriate for this step.

14.7 Configuring Server Migration Targets

The fifth step is to configure server migration targets. You first assign all the available nodes for the cluster’s members and then specify candidate machines (in order of preference) for each server that is configured with server migration. Follow these steps to configure cluster migration in a migration in a cluster:

1. Log in to the WebLogic Server Administration Console (http://Host:Admin_Port/console). Typically, Admin_Port is 7001 by default.
2. In the Domain Structure window, expand Environment and select Clusters.
3. On the Summary of Clusters page, click the cluster for which you want to configure migration (CLUSTER) in the Name column of the table.

   **Note:** For the procedures in this document, configure server migration for the Oracle SOA Suite and Imaging clusters.
4. Open 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 **HOST1** and **HOST2**.

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. Click **Lock & Edit**.

11. Set the candidate machines for server migration. You must perform this task for all of the managed servers as follows:

   a. In the Domain Structure window of the WebLogic Server Administration Console, expand **Environment** and select **Servers**.

   b. Select the server for which you want to configure migration.

   c. Open 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_SERVER1**, select **HOST2**. For **WLS_SERVER2**, select **HOST1**.

   e. Select **Automatic Server Migration Enabled**. This enables Node Manager to start a failed server on the target node automatically.

   f. Click **Save**.

   g. Click **Activate Changes**.

   h. Restart the Administration Server, node managers, and the servers for which server migration has been configured.

---

**Note:** For the procedures in this document, configure server migration for the Oracle SOA Suite and Imaging servers.

---

**14.8 Testing the Server Migration**

The sixth and final step is to test the server migration. To verify that server migration is working properly:

**From **HOST1**:  

1. Stop the **WLS_SERVER1** managed server. To do this, run this command on **HOST1**:

   ```bash
   kill -9 pid
   ```

   where **pid** specifies the process ID of the managed server. You can identify the pid in the node by running this command:

   ```bash
   ps -ef | grep WLS_SERVER1
   ```

2. Watch the Node Manager console. You should see a message indicating that **WLS_SERVER1**'s floating IP has been disabled.
3. Wait for Node Manager to try a second restart of `WLS_SERVER1`. It waits for a fence period of 30 seconds before trying this restart.

4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

From `HOST2`:
1. Watch the local Node Manager console. After 30 seconds since the last try to restart `WLS_SERVER1` on node 1, Node Manager on node 2 should prompt that the floating IP for `WLS_SERVER1` 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
Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.

2. Click `Domain` on the left console.

3. Open the `Monitoring` tab and then the `Migration` subtab.

   The Migration Status tab provides information on the status of the migration (Figure 14–1).

*Figure 14–1  Migration Status Screen in the Administration Console*
Note: After a server is migrated, to fail it back to its original node or machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.
This chapter describes how to integrate Oracle WebCenter Content with Oracle Identity Management. It contains the following sections:

- Section 15.1, "Overview of Integrating with Oracle Identity Management”
- Section 15.2, "Credential and Policy Store Configuration”
- Section 15.3, "Oracle Access Manager 10g Integration”
- Section 15.4, "Oracle Access Manager 11g Integration”
- Section 15.5, "Validating Access Through Oracle HTTP Server and SSO”
- Section 15.6, "Backing Up the Installation”

15.1 Overview of Integrating with Oracle Identity Management

You can integrate an Oracle Fusion Middleware enterprise deployment with Oracle Identity Management 10g or 11g. The following sections describe how to first configure credential and policy stores, reassociate those credential and policy stores, and then integrate with Oracle Identity Management 10g or 11g.

**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 lists the high-level steps for integrating Oracle Identity Management 10g with an Oracle WebCenter Content enterprise deployment.
Table 15–1  **Steps for Integrating with Oracle Identity Management 10g**  

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the credential store</td>
<td>Configure the Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Content enterprise deployment topology.</td>
<td>Section 15.2, &quot;Credential and Policy Store Configuration&quot;</td>
</tr>
<tr>
<td>Configure the policy store</td>
<td>Configure the Oracle Internet Directory LDAP as the policy store for the Oracle WebCenter Content enterprise deployment topology.</td>
<td>Section 15.2.3, &quot;Policy Store Configuration&quot;</td>
</tr>
<tr>
<td>Run the OAM Configuration Tool</td>
<td>The OAM Configuration Tool (oamcfg) starts a series of scripts and sets up the required policies.</td>
<td>Section 15.3.2, &quot;Running the OAM Configuration Tool&quot;</td>
</tr>
<tr>
<td>Install and configure WebGate</td>
<td>Install WebGate on each of the WEBHOST machines to secure the Web tier.</td>
<td>Section 15.3.4, &quot;Installing and Configuring WebGate&quot;</td>
</tr>
<tr>
<td>Configure IP validation for the Webgate</td>
<td>Configure the IP validation for the Webgate using Access System Console.</td>
<td>Section 15.3.5, &quot;Configuring IP Validation for the Enterprise Deployment Webgate&quot;</td>
</tr>
<tr>
<td>Set up WebLogic Server authenticators</td>
<td>Set up the WebLogic Server authenticators by backing up the configuration files, setting up the Oracle Access Manager ID Asserter, and setting the order of providers.</td>
<td>Section 15.3.6, &quot;Setting Up WebLogic Server Authenticators&quot;</td>
</tr>
</tbody>
</table>

Table 15–2 lists the high-level steps for integrating Oracle Identity Management 11g with an Oracle WebCenter Content enterprise deployment.

Table 15–2  **Steps for Integrating with Oracle Identity Management 11g**  

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the credential store</td>
<td>Configure the Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Content Enterprise Deployment topology.</td>
<td>Section 15.2, &quot;Credential and Policy Store Configuration&quot;</td>
</tr>
<tr>
<td>Configure the policy store</td>
<td>Configure the Oracle Internet Directory LDAP as the policy store for the Oracle WebCenter Content Enterprise Deployment topology.</td>
<td>Section 15.2.3, &quot;Policy Store Configuration&quot;</td>
</tr>
<tr>
<td>Install WebGate</td>
<td>Install WebGate on each of the WEBHOST machines where an HTTP Server has already been installed.</td>
<td>Section 15.3.4, &quot;Installing and Configuring WebGate&quot;</td>
</tr>
<tr>
<td>Register the WebGate agent</td>
<td>Register the Webgate agent using the RREG tool.</td>
<td>Section 15.4.4, &quot;Registering the WebGate Agent&quot;</td>
</tr>
<tr>
<td>Set up WebLogic Server authenticators</td>
<td>Set up the WebLogic Server authenticators by backing up the configuration files, setting up the Oracle Access Manager ID Asserter, and setting the order of providers.</td>
<td>Section 15.3.6, &quot;Setting Up WebLogic Server Authenticators&quot;</td>
</tr>
</tbody>
</table>
15.2 Credential and Policy Store Configuration

The following topics describe credential and policy store configuration in detail:

- Section 15.2.1, "Overview of Credential and Policy Store Configuration"
- Section 15.2.2, "Credential Store Configuration"
- Section 15.2.3, "Policy Store Configuration"
- Section 15.2.4, "Reassociation of Credentials and Policies"

15.2.1 Overview of Credential and Policy Store Configuration

Oracle Fusion Middleware allows using different types of credential and policy stores in an Oracle WebLogic Server 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 enterprise deployment topology for Oracle WebCenter Content uses different domain homes for the Administration Server and the managed servers, which means that Oracle requires the use of an LDAP store as policy and credential store for integrity and consistency. By default, 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 reassociation of both the credential and the policy stores is accomplished as a unit using the Fusion Middleware Control or the WLST command `reassociateSecurityStore`. For more information, see Section 15.2.4, "Reassociation of Credentials and Policies."

---

15.2.2 Credential Store Configuration

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. This section provides steps to configure Oracle Internet Directory LDAP as a credential store for the Oracle WebCenter Content enterprise deployment topology. For more details on credential store configuration, see the "Configuring the Credential Store" chapter in the *Oracle Fusion Middleware Security Guide*.

The following section describe credential store configuration:

- Section 15.2.2.1, "Creating the LDAP Authenticator"
- Section 15.2.2.2, "Moving the WebLogic Server Administrator to LDAP"
- Section 15.2.2.3, "Reassociating the Domain Credential Store"
15.2.2.1 Creating the LDAP Authenticator

To be safe, before you create the LDAP authenticator, you should first 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

Also back up the boot properties file for the Administration Server:

- ORACLE_BASE/admin/domain_name/aserver/domain_name/servers/AdminServer/security/boot.properties

Follow these steps to set the proper authenticator:

1. Log in to the Oracle WebLogic Server Administration 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.
10. Click OK.
11. In the Providers screen, click the newly created Authenticator.
12. 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.
13. Click Save to save this setting.
14. Open the Provider Specific tab to enter the details for the LDAP server.
15. Enter the details specific to your LDAP server, as shown in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Value Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>For example: oid.mycompany.com</td>
<td>The LDAP server's server ID.</td>
</tr>
<tr>
<td>Port</td>
<td>For example: 636</td>
<td>The LDAP server's port number.</td>
</tr>
<tr>
<td>Principal</td>
<td>For example: cn=orcladmin</td>
<td>The LDAP user DN used to connect to the LDAP server.</td>
</tr>
<tr>
<td>Credential</td>
<td>NA</td>
<td>The password used to connect to the LDAP server.</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Checked</td>
<td>Specifies whether SSL protocol is used when connecting to LDAP server.</td>
</tr>
<tr>
<td>User Base DN</td>
<td>For example: cn=users,dc=us, dc=mycompany,dc=com</td>
<td>Specify the DN under which your Users start.</td>
</tr>
<tr>
<td>Group Base DN</td>
<td>For example: cn=groups,dc=us, dc=mycompany,dc=com</td>
<td>Specify the DN that points to your Groups node.</td>
</tr>
<tr>
<td>Use Retrieved User Name as Principal</td>
<td>Checked</td>
<td>Must be turned on.</td>
</tr>
</tbody>
</table>

Click Save when done.

16. Click Activate Changes to propagate the changes.

15.2.2.1.1 Setting the Order of Providers  Reorder the OID/OVD Authenticator and Default Authenticator and ensure that the control flag for each authenticator is set in the following order:

- OID LDAP Authenticator: SUFFICIENT
- Default Authenticator: SUFFICIENT

To set the order of providers:

1. Log in to the WebLogic Server Administration 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.
15.2.2.2 Moving the WebLogic Server Administrator to LDAP

This section provides details for provisioning a new administrator user and group for managing the Oracle WebCenter Content WebLogic Server domain in the enterprise deployment topology. This section describes the following tasks:

- Section 15.2.2.2.1, "Provisioning Admin Users and Groups in an LDAP Directory"
- Section 15.2.2.2.2, "Assigning the Admin Role to the Admin Group"
- Section 15.2.2.2.3, "Updating the boot.properties File and Restarting the System"

15.2.2.2.1 Provisioning Admin Users and Groups in an LDAP Directory

As mentioned in the introduction to this section, users and groups from multiple WebLogic Server domains may be provisioned in a central LDAP user store. In such a case, there is a possibility that one WebLogic Server administration user may have access to all the domains within an enterprise. This is not a desirable situation. To avoid this, the users and groups provisioned must have a unique, distinguished name within the directory tree. In this guide, the administration user and group for the Oracle WebCenter Content WebLogic Server domain will be provisioned with the following DNs:

- Admin User DN:
  
  cn=weblogic_ecm,cn=Users,dc=us,dc=mycompany,dc=com

- Admin Group DN:
  
  cn=ECM Administrators,cn=Groups,dc=us,dc=mycompany,dc=com

Follow these steps to provision the admin user and admin group in Oracle Internet Directory:

1. Create an LDIF file named admin_user.ldif with the following contents, depending on the Oracle Access Manager version used, and then save the file:

   - **Oracle Access Manager 10g**:
     
     dn: cn=weblogic_ecm, cn=Users, dc=us, dc=mycompany, dc=com
     orclsamaccountname: weblogic_ecm
     givenname: weblogic_ecm
     sn: weblogic_ecm
     userpassword: Welcome1
     mail: weblogic_ecm
     objectclass: top
     objectclass: person
     objectclass: organizationalPerson
     objectclass: inetorgperson
     objectclass: orcluser
     objectclass: orcluserV2
     uid: weblogic_ecm
     cn: weblogic_ecm
     description: Admin User for the Oracle WebCenter Content Domain

   - **Oracle Access Manager 11g**:
     
     dn: cn=weblogic_ecm, cn=Users, dc=us, dc=mycompany, dc=com
     orclsamaccountname: weblogic_ecm
     givenname: weblogic_ecm
     sn: weblogic_ecm
     userpassword: Welcome1
     mail: weblogic_ecm
     objectclass: top
     objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
uid: weblogic_ecm
cn: weblogic_ecm
description: Admin User for the Oracle WebCenter Content Domain

2. Run the **ldapadd** command on the Oracle Internet Directory host 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 Oracle Identity Management installation where Oracle Internet Directory resides.

   For example (all on a single line):

   ```
   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=ECM Administrators, cn=Groups, dc=us, dc=mycompany, dc=com
displayname: ECM Administrators
   objectclass: top
   objectclass: groupOfUniqueNames
   objectclass: orclGroup
   uniquemember: cn=weblogic_ecm, cn=users, dc=us, dc=mycompany, dc=com
cn: ECM Administrators
description: Administrators Group for the Oracle WebCenter Content Domain
   ```

4. Run the **ldapadd** command on the Oracle Internet Directory host located under the **ORACLE_HOME/bin** directory to provision the group in Oracle Internet Directory (all on a single line):

   ```
   ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w welcome1 -c -v -f admin_group.ldif
   ```

15.2.2.2.2 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 Server domain security realm. This enables all users that belong to the group to be administrators for that domain. Follow these steps to assign the Admin role to the Admin group:

1. Log in to the WebLogic Administration Server Console.

2. In the left pane of the console, click **Security Realms**.

3. On the Summary of Security Realms page, click **myrealm** under the Realms table.

4. On the Settings page for myrealm, open 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 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 ECM Administrators in the Group Argument field and click Add.

7. Click Finish to return to the Edit Global Rule page.

8. The Role Conditions table now shows the ECM Administrators Group as an entry.

9. Click Save to finish adding the Admin Role to the ECM Administrators Group.

10. Validate that the changes were successful by bringing up the WebLogic Server Administration Console using a web browser. Log in using the credentials for the weblogic_ecm user.

   **Note:** Each Oracle application in the Oracle WebCenter Content enterprise deployment topology may have its own predefined roles and groups defined for administration and monitoring purposes. By default, the Administrators group will allow these operations. However, this group may be too broad. For example, it may be undesirable that Oracle SOA Suite administrators are also administrators for the WebLogic Server domain where Oracle SOA Suite, Oracle WebCenter Content, and Oracle WebCenter Content: Imaging are running. This is why it may be desirable, as suggested in this section, to create a more specific group such as ECM Administrators. For the various applications to allow the ECM Administrators group to administer the different systems, you need to add the required roles to that group. For example, for SOA Worklistapp's administration, add the SOAAdmin role. Refer to each component's specific roles for the required roles in each case.

---

15.2.2.2.3 Updating the boot.properties File and Restarting the System

The boot.properties file for the Administration Server should be updated with the WebLogic Server administration user created in Oracle Internet Directory. Follow these steps to update the boot.properties file:

1. On SOAHOST1, go the following directory:
   ```
   cd ORACLE_BASE/admin/domain_name/aserver/domain_name/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_ecm
   password=welcome1
   ```
4. Save the file.
5. Stop the Administration Server using the following command:

   \texttt{wls:/nm/domain\_name}\texttt{\textbackslash{}nmKill(\textquoteleft\textquoteleft AdminServer\textquoteright\textquoteleft\textquoteleft)}

6. Start the Administrator Server using the procedure in Section 8.4.4, "Starting the Administration Server on SOAHOST1."

15.2.2.3 Reassociating the Domain Credential Store

The reassociation of both the credential and the policy stores is accomplished as a unit using Fusion Middleware Control or the WLST command \texttt{reassociateSecurityStore}. See Section 15.2.4, "Reassociation of Credentials and Policies" for detailed steps.

15.2.3 Policy Store Configuration

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 WebCenter Content enterprise deployment topology. For more details on policy store configuration, refer to the "OPSS Authorization and the Policy Store" chapter in the \textit{Oracle Fusion Middleware Security Guide}.

15.2.3.1 Prerequisites to Using an LDAP-Based Policy Store

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. An Oracle Internet Directory administrator must follow these steps to create the appropriate node in an Oracle Internet Directory Server:

1. Create an LDIF file (assumed to be \texttt{jpstestnode.ldif} in this example) specifying the following DN and CN entries:

   \texttt{dn: cn=jpsroot\_ecm}
   \texttt{cn: jpsroot\_ecm}
   \texttt{objectclass: top}
   \texttt{objectclass: OrclContainer}

   The distinguished name of the root node (illustrated by the string \texttt{jpsroot\_ecm} above) must be distinct from any other distinguished name. One root node can be shared by multiple WebLogic Server 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 \texttt{ldapadd} command on the OID server, as illustrated in the following example (all on a single line):

   \texttt{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 \texttt{ldapsearch} command on the Oracle Internet Directory server, as illustrated in the following example (all on a single line):

   \texttt{ORACLE\_HOME/bin/ldapsearch -h ldap\_host -p ldap\_port -D cn=orcladmin -w password -h "cn=jpsroot\_ecm" objectclass="orclContainer"}
4. When using Oracle Internet Directory as the LDAP-based policy store, run the oidstats.sql utility in the INFRADBBHOST servers to generate database statistics for optimal database performance:

```
ORACLE_HOME/bin/sqplus
```

Enter ODS as a user name. You will be prompted for credentials for the ODS user. Inside SQL*Plus, enter the command to gather the statistics info:

```
@ORACLE_HOME/ldap/admin/oidstats.sql
```

The oidstats.sql utility must be run just once after the initial provisioning. For details about this utility, consult the Oracle Fusion Middleware User Reference for Oracle Identity Management.

### 15.2.3.2 Reassociating the Domain Policy Store

Reassociating the policy store consists in migrating policy data from a file-based or LDAP-based repository to an LDAP-based repository; that is, reassociation changes the repository preserving the integrity of the data stored. For each policy in the source policy store, reassociation searches the target LDAP directory and, if it finds a match, it updates the matching policy as appropriate. If none is found, it simply migrates the policy as is.

At any time, after a domain policy store has been instantiated, a file-based 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.

The reassociation of both the credential and the policy stores is accomplished as a unit using Oracle Enterprise Manager Fusion Middleware Control or the WLST reassociateSecurityStore command. See Section 15.2.4, “Reassociation of Credentials and Policies” for detailed steps.

### 15.2.4 Reassociation of Credentials and Policies

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST reassociateSecurityStore command. Follow these steps:

1. From SOAHOST1, start the wlst shell:
   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./wlst.sh
   ```

2. Connect to the WebLogic Server Administration Server using the following wlst connect command.
   Syntax:
   ```
   connect("Admin_User","Admin_User_Password","t3://hostname:port")
   ```
   For example:
   ```
   connect("weblogic","welcome1","t3://ADMINVHN:7001")
   ```
3. Run the `reassociateSecurityStore` command as shown below:

   Syntax:
   
   ```
   reassociateSecurityStore(domain="domain_name", admin="cn=orcladmin", password="orclPassword", ldapurl="ldap://LDAP_HOST:LDAP_PORT", servertype="OID", jpsroot="cn=jpsroot_ecm")
   ```
   
   For example:
   
   ```
   wls:/domain_name/serverConfig>reassociateSecurityStore(domain="domain_name", admin="cn=orcladmin", password="welcome1", ldapurl="ldap://oid.mycompany.com:389", servertype="OID", jpsroot="cn=jpsroot_ecm")
   ```
   
   The output for the command is shown below:
   
   ```
   {servertype=OID,jpsroot_ecm=cn=jpsroot_ecm_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 the 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
   Starting keystore reassociation
   The server and ServiceConfigurator setup done.
   Schema is seeded into the server
   Data is migrated to the server
   Service in the server after migration has been tested to be available
   Update of jps configuration is done
   keystore 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 8.4.4, "Starting the Administration Server on SOAHOST1."

   **Note:** For credential and policy changes to take effect, the servers in the domain must be restarted.

15.2.4.1 Cataloging Oracle Internet Directory Attributes

An Oracle Internet Directory attribute used in a search filter must be indexed. The indexing is an optional procedure used to enhance performance. If not done yet in this OID, use the `catalog` tool to index attributes:

```
catalog connect="orcl" add=true attribute="orclrolescope" verbose="true"
```
Optionally, the attribute names can be placed in a file and processed in a batch as follows:

- orclrolescope
- orclassignedroles
- orclApplicationCommonName
- orclAppName
- orclCSFAlias
- orclCSFKey
- orclCSFName
- orclCSFDDBUrl
- orclCSFDDBPort
- orclCSFCredentialType
- orclCSFExpiryTime
- modifytimestamp
- createtimestamp
- orcljpsassignee

For more information on indexing OID attributes, see the Oracle Fusion Middleware Reference for Oracle Identity Management.

### 15.3 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 Content enterprise deployment topology. It contains the following sections:

- Section 15.3.1, "Overview of Oracle Access Manager Integration"
- Section 15.3.2, "Prerequisites for Oracle Access Manager"
- Section 15.3.3, "Configuring Oracle Access Manager"
- Section 15.3.4, "Installing and Configuring WebGate"
- Section 15.3.5, "Configuring IP Validation for the Enterprise Deployment Webgate"
- Section 15.3.6, "Setting Up WebLogic Server Authenticators"

#### 15.3.1 Overview of Oracle Access Manager Integration

Oracle Access Manager is the recommended single sign-on (SSO) solution for Oracle Fusion Middleware 11g Release 1. For more information on installing and configuring an Oracle Access Manager installation, see Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management. This section explains the procedure for configuring the Oracle WebCenter Content installation with an existing Oracle Access Manager 10g installation and the underlying directory service. Oracle recommends using either Oracle Internet Directory or Oracle Virtual Directory or both of these directory services.

**Note:** The Oracle WebCenter Content enterprise deployment topology described in this book uses a single sign-on configuration where both the Oracle WebCenter Content system and the single sign-on system are in the same network domain (mycompany.com). For a multidomain configuration, see the required configuration steps in "Configuring Single Sign-On" in the Oracle Access Manager Access Administration Guide.
15.3.2 Prerequisites for Oracle Access Manager

The setup for Oracle Access Manager assumes an existing Oracle Access Manager 10g installation complete with Access Managers and a policy protecting the Policy Manager. For more information on installing and configuring an Oracle Access Manager installation, see Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management. This setup includes a directory service such as Oracle Internet Directory, either stand-alone or as part of an Oracle Virtual Directory configuration. This section provides the necessary steps for configuring your enterprise deployment with either Oracle Internet Directory or Oracle Virtual Directory.

In addition, the Oracle Access Manager installation should have its own Web server configured with WebGate. This section also provides the steps for using the Oracle Access Manager Web server as a delegated authentication server.

15.3.3 Configuring Oracle Access Manager

This section covers the following topics:

- Section 15.3.3.1, "Collecting the Information for the OAM Configuration Tool"
- Section 15.3.3.2, "Running the OAM Configuration Tool"
- Section 15.3.3.3, "Oracle Access Manager Logout Guidelines"
- Section 15.3.3.4, "Verifying Successful Creation of the Policy Domain and AccessGate"
- Section 15.3.3.5, "Verifying That the Cookieless Basic Authorization Scheme Has Been Properly Assigned"
- Section 15.3.3.6, "Updating the Host Identifier"
- Section 15.3.3.7, "Updating the WebGate Profile"
- Section 15.3.3.8, "Adding Additional Access Servers"
- Section 15.3.3.9, "Configuring Delegated Form Authentication"

15.3.3.1 Collecting the Information for the OAM Configuration Tool

The OAM Configuration Tool (oamcfg) starts a series of scripts and sets up the required policies for Oracle Access Manager. It requires various parameters as inputs. Specifically, it creates the following:

1. A form authentication scheme in Oracle Access Manager
2. Policies to enable authentication in WebLogic Server
3. A WebGate entry in Oracle Access Manager 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. A host identifier, depending on the scenario chosen (a default host identifier would be used, if not provided)
6. Policies to protect and unprotect application specific URLs.
The following information should be collected or prepared prior to running the OAM Configuration Tool:

1. **Password**: Create a secure password. This will be used as the password for the WebGate installation created later.

2. **LDAP Host**: host name of the directory server or load balancer address in the case of a high-availability or enterprise deployment configuration.

3. **LDAP Port**: port of the directory server.

4. **LDAP USER DN**: DN of the LDAP admin user. This will be a value such as cn=orcladmin.

5. **LDAP password**: password of the LDAP admin user.

6. **oam_aaa_host**: host name of an Oracle Access Manager.

7. **oam_aaa_port**: port of the Oracle Access Manager.

### 15.3.3.2 Running the OAM Configuration Tool

Before running the OAM Configuration Tool, you must first add the required resources to Oracle Access Manager 10g for the Oracle WebCenter Content components. Create a file containing the list of URIs you want to protect with the following content:

```
#########################################
#Product Name: Oracle WebCenter Content
#########################################
#########################################
protected_uris
#########################################
/ADFAuthentication
/imaging/faces
/em
/console
/DefaultToDoTaskFlow
/sdpmessaging/userprefs-ui
/integration/worklistapp
/workflow/sdpmessagingasca-ui-worklist
/soa/composer
/soa-infra/deployer
/soa-infra/events/edn-db-log
/soa-infra/cluster/info

#"Policy using Basic Authn Scheme" is the name of the policy
#"Basic Over LDAP" is the authentication scheme configured for this #policy
# Note that the name of the policy and the scheme name in the URIs file
# is tab-separated. In other words, there must be a tab between
# "Basic Authn Scheme" and "OraDefaultBasicAuthNScheme" below.
Policy using Basic Authn Scheme OraDefaultBasicAuthNScheme
/inspection.wsil

#########################################
#########################################
public_uris
#########################################
/soa-infra/services
/soa-infra/directWSDL
```

---

### 15-14 Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Content
The OAM Configuration Tool resides in the ORACLE_COMMON_HOME/modules/oracle.oamprovider_11.1.1 directory (ORACLE_COMMON_HOME depends on the machine where you are running the configuration tool). The tool can be run from any machine with the required installation files. In this case, we run it from WCCHOST1. Run the OAM Configuration Tool for Oracle Access Manager 10g registration as follows (all on a single command line):

```java
MW_HOME/jrockit_160_version/bin/java -jar oamcfgtool.jar mode=CREATE
app_domain="ECM_EDG"
uris_file="full_path_to_file_containing_uri_definitions"
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=OAMPORT1
```

If your command ran successfully, you should see the following output:

```
Date,Time oracle.security.oam.oamcfg.OAMCfgGlobalConfigHandler
constructGlobalConfig
INFO: Processed input parameters
May 9, 2011 5:09:40 AM oracle.security.oam.oamcfg.OAMCfgGlobalConfigHandler
constructGlobalConfig
INFO: Initialized Global Configuration
Date,Time oracle.security.oam.oamcfg.create.impl.OAMCfgConfigCreator doCreate
INFO: Successfully completed the Create operation.
Date,Time oracle.security.oam.oamcfg.create.impl.OAMCfgConfigCreator doCreate
INFO: Operation Summary:
Date,Time oracle.security.oam.oamcfg.create.impl.OAMCfgConfigCreator doCreate
INFO:      Policy Domain  : ECM_EDG
Date,Time oracle.security.oam.oamcfg.create.impl.OAMCfgConfigCreator doCreate
INFO:      Host Identifier: ECM_EDG
Date,Time oracle.security.oam.oamcfg.create.impl.OAMCfgConfigCreator doCreate
INFO:      Access Gate ID : ECM_EDG_AG
```

15.3.3.3 Oracle Access Manager Logout Guidelines

For applications invoked by Oracle WebCenter Content and Oracle WebCenter Content: Imaging to comply with Oracle Access Manager logout guidelines (in particular, applications that invoke a logout through /adfAuthentication?logout=true&end_url=some_URI), integration with an Oracle Access Manager 10g environment requires additional configuration on the WebGate to handle the end_url. Without this additional configuration, you are logged out, but not redirected to the end URL because Oracle Access Manager 10g WebGate does not process end_url. For information about configuration procedures, see Oracle Fusion Middleware Security Guide.
When integrating Oracle WebCenter Content with Oracle Access Manager 10g, you must add the URL /oamsso/logout.html to the logout URL setting for the Access Gate for the single sign-on logout to work properly. See "Configuring a Single Sign-On Logout URL" and "AccessGate Configuration Parameters" in the Oracle Access Manager Access Administration Guide for more information.

15.3.3.4 Verifying Successful Creation of the Policy Domain and AccessGate

Verifying the Policy Domain
To verify the policy domain:

1. Log in to Oracle Access Manager:
   
   http://OAMADMINHOST:port/access/oblix/

2. Click Policy Manager.

3. Click the My Policy Domains link on the left panel. You will see a list of all policy domains, which includes the domain you just created. It will have the suffix _PD (for example, ECM_EDG_PD). In the third column (URL prefixes), you will also see the URIs you specified during the creation of this domain.

4. Click the link to the policy domain you just created to go to the General area of this domain.

5. Open the Resources tab and you will see the URIs you specified. You can also click other tabs to view other settings.

Verifying the AccessGate Configuration
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. Open the Access System Configuration tab.

3. Click the AccessGate Configuration link on the left panel.

4. Enter ECM_EDG as the search criterion (or any other substring you may have used as the app_domain name in Section 15.3.3.2, "Running the OAM Configuration Tool"), and click Go.

5. Once the access gate for the domain you just created shows up (this will have the suffix _AG (for example, ECM_EDG_AG), click it, and you will see the details of the access gate you just created.

15.3.3.5 Verifying That the Cookieless Basic Authorization Scheme Has Been Properly Assigned
To verify that the cookieless basic authorization scheme has been properly assigned:

1. Log in to Oracle Access Manager:
   
   http://OAMADMINHOST:port/access/oblix/

2. Click Policy Manager.

3. Click the My Policy Domains link on the left panel. You will see a list of all policy domains that have been created.

4. Click ECM_EDG.
5. Open the **Policies** tab and then click **Policy using Basic Authn Scheme**.

6. Open the **General** section.
   The inspection.wsil resource should be listed.

7. Open the **Authentication Rule** section.
   The OraDefaultBasicAuthNScheme authentication scheme should be listed.

### 15.3.3.6 Updating the Host Identifier

The OAM Configuration Tool uses the value of the `app_domain` parameter to create a host identifier for the policy domain. This host identifier must be updated with all the host name variations for the host so that the configuration works correctly.

To update the host identifier created by the OAM Configuration Tool:

1. Navigate to the Access System Console by specifying the following URL in your web browser:

   \[http://host_name:port/access/oblix\]

   where `host_name` 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. When prompted for a user name 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, open 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 the host identifier created by the OAM Configuration Tool (for example, **ECM_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
   - soahost1vhn1.mycompany.com:8001
   - soahost2vhn1.mycompany.com:8001
   - soainternal.mycompany.com:80
   - wcchost1vhn1.mycompany.com:16000
   - wcchost2vhn1.mycompany.com:16000
   - wcchost1.mycompany.com:16200
   - wcchost2.mycompany.com:16200
   - wcc.mycompany.com:443
   - wccinternal.mycompany.com:80
   - admin.mycompany.com:80
   - adminvhn.mycompany.com:7001
   - sso.mycompany.com:7779 [WebGate access with Oracle IDM port]
9. Select the **Update Cache** checkbox, 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.

### 15.3.3.7 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.

To update the WebGate profile created by the OAM Configuration Tool:

1. Navigate to the Access System Console by specifying the following URL in your web browser:

   ```
   http://host_name:port/access/oblix
   ```

   where **host_name** 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, 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 in the left pane to display the AccessGates Search page.

4. Enter the proper search criteria and click **Go** to display a list of access gates.

5. Select the access gate created by the OAM Configuration Tool (for example, **ECM_EDG_AG**).

6. On the AccessGate Details page, select **Modify** to display the Modify AccessGate page.

7. On the Modify AccessGate page, update the following:

   - **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 following message is displayed: *Are you sure you want to commit these changes?*

   Click **OK** to finish updating the configuration.

9. Verify the values displayed on the Details for AccessGate page to confirm that the updates were successful.
15.3.3.8 Adding Additional Access Servers
To assign an access server to the WebGate:

1. Log in as the Administrator on the Access System Console.

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 (ECM_EDG_AG).


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 define two connections for the WebGate. Click the Add button to complete the association.

6. A page appears, showing the association of the Access Server with the WebGate. Click the link to display a summary and print this page for later use.

7. Repeat steps 3 through 6 to associate more access servers to the WebGate.

15.3.3.9 Configuring Delegated Form Authentication
To configure the form authentication to redirect to the WebGate that was installed with the Oracle Access Manager 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 IDM installation; for example: http://sso.mycompany.com. Click Save when you are done.

A WebGate should already be installed in the IDM installation. Refer to Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management for details.
15.3.4 Installing and Configuring WebGate

WebGate needs to be installed on both WEBHOST1 and WEBHOST2 to secure the web tier:

---

**Note:** There is a known issue with the Oracle Access Manager installer that sometimes manifests as a hang at install time on Linux. This is a third-party issue caused by InstallShield. To work around this issue, follow these steps:

1. Copy and paste the following in the shell where you start the installer:
   ```bash
   cd /tmp
   mkdir bin.$$  
   cd bin.$$  
   cat > mount <<EOF
   #!/bin/sh
   exec /bin/true
   EOF
   chmod 755 mount
   export PATH=`pwd`:$PATH
   
   2. Run the installation.
   3. When the installer is finished running, clean the temporary directory using this command:
      ```bash
      rm -r /tmp/bin.$$  
      ```

---

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 on WEBHOSTn:
   ```bash
   ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g/WebGate -gui
   ```

2. In the Welcome screen, 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.
4. In the installation target screen (Figure 15–2), specify the directory where WebGate should be installed. Click Next to continue.

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.
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 15–3  Runtime Libraries Screen

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 Oracle Access Manager Access Server configuration
- **Access Server host name**, as reported by the Oracle Access Manager Access Server configuration
- **Access Server port number**, as reported by the Oracle Access Manager 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_Component_Name
```

For example:

```
/u01/app/oracle/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.

15.3.5 Configuring IP Validation for the Enterprise Deployment Webgate

IP validation determines if a client’s IP address is the same as the IP address stored in the ObSSOCookie cookie 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 balancing router (LBR) or proxy than the one front-ending the enterprise deployment.

To make sure your enterprise deployment’s LBR or proxy are not validated in these cases:

1. Open the Access System Console and log in as an administrator at the following URL:
   
   http://host_name:port/access/oblix
   
   where host_name 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.

3. On the Access System Console main page, click Access System Configuration, and then click the Access Gate Configuration link in the left pane to display the AccessGates Search page.

4. Enter the appropriate search criteria and click Go to display a list of access gates.

5. Select the access gate created by the OAM Configuration Tool.

6. Click Modify at the bottom of the page.

7. In the IPValidationException field, enter the IP address of the load balancer or proxy front-ending the enterprise deployment.

8. Click Save at the bottom of the page.
15.3.6 Setting Up WebLogic Server Authenticators

This section is based on the assumption that you have already set up the LDAP authenticator by following the steps in Section 15.2.2.1, "Creating the LDAP Authenticator." If you have not already created the LDAP authenticator, do it before continuing with this section.

This section covers the following topics:

- Section 15.3.6.1, "Back Up Configuration Files"
- Section 15.3.6.2, "Setting Up the Oracle Access Manager Identity Asserter"
- Section 15.3.6.3, "Setting the Order of Providers"

15.3.6.1 Back Up Configuration Files

To be safe, first back up the relevant configuration files:

```
ORACLE_BASE/admin/domain_name/aserver/domain_name/config/config.xml
ORACLE_BASE/admin/domain_name/aserver/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.

15.3.6.2 Setting Up the Oracle Access Manager Identity Asserter

To set up the Oracle Access Manager Identity Asserter:

1. Log in to the WebLogic Server Administration Console, if not already logged in.
2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, then the default realm name, and then **Providers**.
4. Click **New** and select **OAMIdentityAsserter** from the dropdown menu.
5. Name the asserter (for example, **OAM ID Asserter**) and click **OK**.
6. Click the newly added asserter to see the configuration screen for the Oracle Access Manager Identity Asserter.
7. Set the control flag to **REQUIRED** and click **Save**.
8. Open the **Provider Specific** tab to configure the following required settings:
   - **Primary Access Server**: provide Oracle Access Manager server endpoint information in `host:port` format.
   - **AccessGate Name**: name of the AccessGate (for example, **ECM_EDG_AG**).
   - **AccessGate Password**: password for the AccessGate (optional).
9. Save the settings.

15.3.6.3 Setting the Order of Providers

Reorder the Oracle Access Manager Identity Asserter, the Oracle Internet Directory or Oracle Virtual Directory Authenticator, and the 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
DefaultIdentityAsserter

After reordering, save the settings, activate the changes, and restart all servers.

---

**Note:** Do not forget to create a new credential for the new user. See Section 11.17, "Configuring BPEL CSF Credentials" for further details. (This book uses the weblogic_ecm user as an example for SSO.)

---

### 15.4 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 Content enterprise deployment topology. It contains the following sections:

- Section 15.4.1, "Overview of Oracle Access Manager Integration"
- Section 15.4.2, "Prerequisites for Oracle Access Manager"
- Section 15.4.3, "Setting Up WebGate"
- Section 15.4.4, "Registering the WebGate Agent"
- Section 15.4.5, "Setting Up the WebLogic Server Authenticators"

#### 15.4.1 Overview of Oracle Access Manager Integration

Oracle Access Manager is the recommended single sign-on solution for Oracle Fusion Middleware 11g Release 1. For more information on installing and configuring an Oracle Access Manager installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This section explains the procedure for configuring the Oracle WebCenter Content installation with an existing Oracle Access Manager 11g 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 Oracle WebCenter Content enterprise deployment topology described in this guide uses a single sign-on configuration where both the Oracle WebCenter Content system and the single sign-on system are in the same network domain (mycompany.com). For a multidomain configuration, see the required configuration steps in "Configuring Single Sign-On" in the *Oracle Access Manager Access Administration Guide*.

---

#### 15.4.2 Prerequisites for Oracle Access Manager

The setup for Oracle Access Manager assumes an existing Oracle Access Manager 11g installation complete with Access Managers and a policy protecting the Policy Manager. For more information on installing and configuring an Oracle Access Manager installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. This setup includes a directory service such as Oracle Internet Directory, either stand-alone or as part of an Oracle Virtual Directory configuration. This section provides the necessary steps for configuring your enterprise deployment with either Oracle Internet Directory or Oracle Virtual Directory.
In addition, the Oracle Access Manager installation should have its own Web server configured with WebGate. This section also provides the steps for using the Oracle Access Manager Web server as a delegated authentication server.

### 15.4.3 Setting Up WebGate

You must set up a WebGate on each of the WEBHOST machines where Oracle HTTP Server has already been installed.

This section covers the following topics:

- Section 15.4.3.1, "Installing GCC Libraries"
- Section 15.4.3.2, "Installing WebGate"
- Section 15.4.3.3, "Post-Installation Steps"

#### 15.4.3.1 Installing GCC Libraries

You must download and install third-party GCC libraries on each of the WEBHOST machines before installing WebGate. You can download the appropriate GCC library from the following third-party web site:

http://gcc.gnu.org

For 32-bit Linux, the required libraries are libgcc_s.so.1 and libstdc++.so.5 with a version number of 3.3.2. Table 15–3 lists the versions of third-party GCC libraries for Linux and Solaris.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>GCC Libraries</th>
<th>Required Library Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 32-bit</td>
<td>x86</td>
<td>libgcc_s.so.1</td>
<td>3.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>libstdc++.so.5</td>
<td></td>
</tr>
<tr>
<td>Linux 64-bit</td>
<td>x64</td>
<td>libgcc_s.so.1</td>
<td>3.4.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>libstdc++.so.6</td>
<td></td>
</tr>
<tr>
<td>Solaris 64-bit</td>
<td>SPARC</td>
<td>libgcc_s.so.1</td>
<td>3.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>libstdc++.so.5</td>
<td></td>
</tr>
</tbody>
</table>

#### 15.4.3.2 Installing WebGate

This section describes the procedures for installing WebGate. You must install WebGate on each of the WEBHOST machines.

**Launching the Installer**

The installer program for Oracle HTTP Server 11g Webgate for Oracle Access Manager is included in the webgate.zip file.

To start the installation wizard:

1. Extract the contents of the webgate.zip file to a directory. By default, this directory is named webgate.
2. Move to the Disk1 subdirectory under the webgate directory.
3. Set the `WEB_HOME` environment variable to the Middleware home for the web tier:

   ```
   export MW_HOME=ORACLE_BASE/product/fmw
   export WEB_HOME=MW_HOME/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 Middleware 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 opens.

### Installation Flow and Procedure

If you need additional help with any of the installation screens, click Help to access the online help.

To install Oracle HTTP Server 11g Webgate for Oracle Access Manager:

1. In the Welcome screen, click **Next**.
2. In the Prerequisite Checks screen, click **Next**.
3. In the Specify Installation Location screen, specify the **Oracle Middleware Home** and **Oracle Home Directory** 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**.
4. In the Specify GCC Library screen, specify the directory that contains the GCC libraries, or click Browse to navigate to their location on your local computer (see Section 15.4.3.1, "Installing GCC Libraries"), and click **Next**.
5. In the Installation Summary screen, verify the information on this screen and click **Install** to begin the installation.
6. 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.
7. In the Installation Complete screen, click **Finish** to exit the installer.

### 15.4.3.3 Post-Installation Steps

Complete the following procedure on each of the WEBHOST machines 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 the Oracle Home for Webgate; for example:

```
MW_HOME/web/Oracle_OAMWebGate1
```

---

**Note:** Oracle_OAMWebGate1 is the default.

---

2. On the command line, run the following command (on a single line) 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
```

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 (on a single line) to copy **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.

---

In the command, **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, for 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** value is the name of the temporary output file used by the tool; for example:

```
Edithttpconf.log
```
15.4.4 Registering the WebGate Agent

This section describes the procedures for registering the WebGate Agent on each of the WEBHOST machines:

- **Section 15.4.4.1, "Extracting and Using the RREG Tool"**
- **Section 15.4.4.2, "Updating the Oracle Access Manager 11g Request File"**
- **Section 15.4.4.3, "Running the oamreg Tool"**
- **Section 15.4.4.4, "Changing the inspection.wsil Resource to Use the Basic Authentication Scheme"**
- **Section 15.4.4.5, "Updating the Oracle Access Manager 11g Server Configuration to Support the Basic Cookieless Scheme"**
- **Section 15.4.4.6, "Copying Access Files to WEBHOST Machines"**

15.4.4.1 Extracting and Using the RREG Tool

The RREG tool is part of the Oracle Access Manager 11g installation. If it is not already available, extract it on each of the WEBHOST machines with 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 -xzf RREG.tar
   ```

3. Edit the oamreg.sh script in the $RREG_HOME/bin directory and change the OAM_REG_HOME parameter according to your setup:

   ```
   OAM_REG_HOME=RREG_Home
   ```

   (where $RREG_Home$ is the directory to which you extracted the contents of RREG.tar.gz and rreg).

   Save the script file.

The RREG Configuration Tool provides a way to register protected, public, and excluded resources into the Oracle Access Manager system. The list of protected resources to be added to the Oracle Access Manager system follows:

- /adfAuthentication
- /adfAuthentication/.../*
- /imaging/faces
- /imaging/faces/.../*
- /em
- /em/.../*
- /console
- /console/.../*
- /DefaultToDoTaskFlow
- /DefaultToDoTaskFlow/.../*
- /sdpmessaging/userprefs-ui
- /sdpmessaging/userprefs-ui/.../*
- /integration/worklistapp
- /integration/worklistapp/.../*
The list of public resources follows:

/cs
/cs/.../*
/_ocsh
/_ocsh/.../*
/imaqing
/imaqing/.../*
/soa-infra/directWSDL
/soa-infra/directWSDL/.../*

The list of excluded resources follows:

/wsm-pm
/wsm-pm/.../*
/soa-infra/services
/soa-infra/services/.../*
/ucs/messaging/webservice

In these lists, "/.../*" implies all resources under the base URL context.

15.4.4.2 Updating the Oracle Access Manager 11g Request File

The REG_HOME/input directory contains a template file named OAM11gRequest.xml. Copy this file to WCCOAM11gRequest.xml, and edit that file to create the policies for the Oracle WebCenter Content installation.

**Note:** Replace OAM_HOST, OAM_ADMINSERVER_PORT, WCC_EDG_AGENT, and WCC_EDG_DOMAIN with their respective values in your installation.
After editing, the file should look as follows:

```xml
<?xml version="1.0" encoding="UTF-8"?>

<OAM11GRegRequest>
  <serverAddress>http://OAM_HOST:OAM_ADMINSERVER_PORT</serverAddress>
  <agentName>WCC_EDG_AGENT</agentName>
  <applicationDomain>WCC_EDG_DOMAIN</applicationDomain>
  <cachePragmaHeader>private</cachePragmaHeader>
  <cacheControlHeader>private</cacheControlHeader>
  <ipValidation>1</ipValidation>
  <ValList ListName="ipValidationExceptions">
    <ValListMember Value="10.1.1.1"/>
  </ValList>
  <logOutUrls>
    <url>/oamsso/logout.html</url>
  </logOutUrls>
  <protectedResourcesList>
    <resource>/adfAuthentication</resource>
    <resource>/imaging/faces</resource>
    <resource>/em</resource>
    <resource>/console</resource>
    <resource>/DefaultToDoTaskFlow</resource>
    <resource>/sdpmessaging/userprefs-ui</resource>
    <resource>/integration/worklistapp</resource>
    <resource>/workflow/sdpmessages-ui-worklist</resource>
    <resource>/soa/composer</resource>
    <resource>/soa-infra</resource>
    <resource>/soa-infra/deployer</resource>
    <resource>/soa-infra/events/edn-db-log</resource>
    <resource>/soa-infra/cluster/info</resource>
    <resource>/inspection.wsiil</resource>
  </protectedResourcesList>
  <publicResourcesList>
    <resource>/cs</resource>
    <resource>_/ocsh</resource>
    <resource>/imaging</resource>
    <resource>/soa-infra/directWSDL</resource>
  </publicResourcesList>
  <excludedResourcesList>
    <resource>/wsm-pm</resource>
    <resource>/soa-infra/services</resource>
    <resource>/ucs/messaging/webservice</resource>
  </excludedResourcesList>
  <userDefinedParameters>
    <userDefinedParam>
      <name>filterOAMAuthnCookie</name>
      <value>false</value>
    </userDefinedParam>
  </userDefinedParameters>
</OAM11GRegRequest>
```
Notes:

- For Oracle Access Manager 11g (11.1.1.2) and later, the `resource_name/.../*` resources will be automatically added during the registration when the request file contains `resource_name/`.

- 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:

  ```xml
  <userDefinedParameters>
  <userDefinedParam>
    <name>ipValidationExceptions</name>
    <value>10.1.1.1</value>
  </userDefinedParam>
  </userDefinedParameters>
  ``

  For more information about adding IP validation exceptions, see the Oracle Fusion Middleware Administrator’s Guide for Oracle Access Manager with Oracle Security Token Service.

15.4.4.3 Running the oamreg Tool

Run the oamreg tool with the following command:

```bash
$ ./RREG_Home/bin/oamreg.sh inband input/WCCOAM11gRequest.xml
```

The run should look as follows:

```
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
  Mode: inband
  Filename: /u01/app/oracle/product/fmw/iam/oam/server/rreg/client/rreg/
            input/WCCOAM11GRequest.xml
  Enter admin username:oamadmin
  Username: your_oamadmin_user
  Enter admin password: your_oamadmin_password
  Do you want to enter a Webgate password?(y/n): y
  Enter webgate password: your_webgate_password
  Enter webgate password again: your_webgate_password
  Password accepted. Proceeding to register...
Apr 18, 2011 12:22:36 PM
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: WCC_EDG_AGENT
  URL String: WCC_EDG_AGENT
  Registering in Mode: inband
  Your registration request is being sent to the Admin server at:
  http://oamserver.mycompany.com:7001
```

Integrating with Oracle Identity Management
Inband registration process completed successfully! Output artifacts are created in the output folder.

15.4.4.4 Changing the inspection.wsil Resource to Use the Basic Authentication Scheme

By default, the inspection.wsil resource is set to use the form authentication scheme. For the connection between the workflow and Oracle WebCenter Content: Imaging to work, this resource must be updated on each of the WEBHOST machines to use the basic authentication scheme instead:

2. Using the navigation tree on the left, choose Application Domains and then the application domain name to navigate to the application domain created (WCC_EDG_DOMAIN).
3. Expand your application domain's name.
5. Double-click Protected Resource Policy.
6. Select the inspection.wsil and inspection.wsil/.../* resources and click the Delete icon in the Resources pane to remove them.
7. Click Apply and confirm the action when prompted.
8. In the navigation tree, click Authentication Policies again, and click the Create button in the tool bar above the navigation tree.
   a. Enter a name for the policy (for example, New Basic Policy).
   b. Select BasicSessionlessScheme as the authentication scheme.
   c. Click Apply.
      You will see the newly created policy under Authentication Policies in the navigation tree.
   d. Open the newly created policy.
   e. On the Resources pane, click the Add icon (plus sign) on the right and add the inspection.wsil and inspection.wsil/.../* resources.
   f. Click Apply.
9. Click the refresh icon on the navigation tree and verify the new authentication policy (click it and make sure the inspection.wsil and inspection.wsil/.../* resources were added).

**Note:** Do not forget to create a new credential for the new user. See Section 11.17, "Configuring BPEL CSF Credentials" for further details. (This book uses the weblogic_ecm user as an example for SSO.)
15.4.4.5 Updating the Oracle Access Manager 11g Server Configuration to Support the Basic Cookieless Scheme

You must set the NoUniqueSessionsFor10gAgents parameter in the Oracle Access Manager 11g configuration to true on each of the WEBHOST machines. To do this, edit the oam-config.xml file located in the IDM_Home/oam/server/config directory and change the line

```xml
<Setting Name="NoUniqueSessionsFor10gAgents" Type="xsd:string">false</Setting>
```

to

```xml
<Setting Name="NoUniqueSessionsFor10gAgents" Type="xsd:string">true</Setting>
```

Save the file, and restart the Oracle Access Manager server in your Oracle Identity Management system for the change to take effect.

15.4.4.6 Copying Access Files to WEBHOST Machines

The following two files are generated in RREG_Home/output/WCC_EDG_AGENT:

- ObAccessClient.xml
- cwallet.sso

Copy these files to the WebGate instance location on each of the WEBHOST machines:

```
scp ObAccessClient.xml oracle@WEBHOSTN:ORACLE_BASE/admin/webN/config/OHS/ohsN/webgate/config/
scp cwallet.sso oracle@WEBHOSTN:ORACLE_BASE/admin/webN/config/OHS/ohsN/webgate/config/
```

In the `scp` command, \( N \) is a sequential number for your installation; for example, 1 for WEBHOST1 or 2 for WEBHOST2.

15.4.5 Setting Up the WebLogic Server Authenticators

This section is based on the assumption that you have already set up the LDAP authenticator by following the steps in Section 15.2.2.1, "Creating the LDAP Authenticator." If you have not already created the LDAP authenticator, do it before continuing with this section.

This section covers the following topics:

- Section 15.4.5.1, "Backing Up Configuration Files"
- Section 15.4.5.2, "Setting Up the Oracle Access Manager Identity Asserter"
- Section 15.4.5.3, "Setting the Order of Providers"

15.4.5.1 Backing Up Configuration Files

To be safe, first 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/fwmconfig/system-jazn-data.xml
```

In addition, back up the boot.properties file for the Administration Server.
### 15.4.5.2 Setting Up the Oracle Access Manager Identity Asserter

To set up the Oracle Access Manager Identity Asserter:

1. Log in to the WebLogic Server Administration Console, if not already logged in.
2. Click **Lock & Edit**.
3. Navigate to **SecurityRealms**, then the default realm name, and then **Providers**.
4. Click **New** and select **OAMIdentityAsserter** from the dropdown menu.
5. Name the asserter (for example, **OAM ID Asserter**) and click **OK**.
6. Click the newly added asserter to see the configuration screen for the Oracle Access Manager 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, and click **Activate Changes** to propagate the changes.

Finally, log in to the WLST console as an administrator and run the following command:

```
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",logouturi="oamsso/logout.html")
```

### 15.4.5.3 Setting the Order of Providers

To set the order of the providers:

1. Log in to the WebLogic Server Administration 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 Oracle Access Manager Identity Asserter, the Oracle Internet Directory or Oracle Virtual Directory Authenticator, and the 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 Validating Access Through Oracle HTTP Server and SSO

Validate single sign-on through both Oracle HTTP Server instances using the following URLs:

- http://WEBHOST1:7777/console
- http://WEBHOST1:7777/em
- http://WEBHOST1:7777/cs
- http://WEBHOST1:7777/imaging
15.6 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. This backup can be discarded 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 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 User’s Guide for information on database backup.

To back up the installation at this point:

1. Back up the web tier:
   a. Shut down the instance using opmnctl:
      ```bash
      ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
      ```
   b. Back up the Middleware home on the web tier using the following command (as root):
      ```bash
      tar -cvpf BACKUP_LOCATION/web.tar $MW_HOME
      ```
   c. Back up the Instance Home on the web tier using the following command (as root):
      ```bash
      tar -cvpf BACKUP_LOCATION/web_instance.tar $ORACLE_INSTANCE
      ```
   d. Start the instance using opmnctl:
      ```bash
      ORACLE_BASE/admin/instance_name/bin/opmnctl startall
      ```

2. Back up the AdminServer domain directory on SOAHOST1. Perform a backup to save your domain configuration. The configuration files all exist under the ORACLE_BASE/admin/domain_name directory.
   ```bash
   tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
   ```
This chapter describes some operations that you can perform after you have set up the topology, including monitoring, scaling, and backing up your topology. It contains the following sections:

- Section 16.1, "Overview of Managing the Oracle WebCenter Content Topology"
- Section 16.2, "Defining an Optimal Input File Strategy for Oracle WebCenter Content: Imaging"
- Section 16.3, "Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology"
- Section 16.4, "Managing Space in the SOA Infrastructure Database"
- Section 16.5, "Configuring UMS Drivers for Oracle WebCenter Content: Imaging"
- Section 16.6, "Scaling Up the Oracle WebCenter Content Topology"
- Section 16.7, "Scaling Out the Oracle WebCenter Content Topology"
- Section 16.8, "Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments"
- Section 16.9, "Preventing Timeouts for SQLNet Connections"
- Section 16.10, "Configuring Oracle Web Service Manager Security Policies for Oracle WebCenter Content and Imaging Services"
- Section 16.11, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology"
16.1 Overview of Managing the Oracle WebCenter Content Topology

After configuring the Oracle WebCenter Content enterprise deployment, you can use the information in this chapter to manage the topology. Table 16–1 lists some tasks you can perform to manage the topology.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage the Oracle SOA Suite subsystem used by Imaging</td>
<td>Deploy SOA composites to a server address, manage space in the Oracle SOA Suite infrastructure, and configure UMS drivers.</td>
<td>Section 16.3, “Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology”; Section 16.4, “Managing Space in the SOA Infrastructure Database”; Section 16.5, “Configuring UMS Drivers for Oracle WebCenter Content: Imaging”</td>
</tr>
<tr>
<td>Expand the topology by scaling it up, or out</td>
<td>Add new managed servers to nodes, or add new nodes.</td>
<td>Section 16.6, “Scaling Up the Oracle WebCenter Content Topology”; Section 16.7, “Scaling Out the Oracle WebCenter Content Topology”</td>
</tr>
<tr>
<td>Back up the topology before and after any configuration changes</td>
<td>Back up directories and files to protect against failure as a result of configuration changes.</td>
<td>Section 16.8, “Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments”</td>
</tr>
<tr>
<td>Prevent connection timeouts</td>
<td>Configure the firewall so that the database connection is not timed out.</td>
<td>Section 16.9, “Preventing Timeouts for SQLNet Connections”</td>
</tr>
<tr>
<td>Configure Oracle Web Services Manager (Oracle WSM) security policies for Oracle WebCenter Content and Imaging web services</td>
<td>Use the appropriate Oracle WSM policy enforcements instead of basic HTTP authentication.</td>
<td>Section 16.10, “Configuring Oracle Web Service Manager Security Policies for Oracle WebCenter Content and Imaging Services”</td>
</tr>
<tr>
<td>Troubleshoot problems</td>
<td>Implement solutions for known issues that may occur after you have configured the topology.</td>
<td>Section 16.11, “Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology”</td>
</tr>
</tbody>
</table>

For more information about managing Oracle WebCenter Content, see the following documents:

- Oracle WebCenter Content System Administrator’s Guide for Content Server
- Oracle WebCenter Content Application Administrator’s Guide for Content Server
- Oracle WebCenter Content Administrator’s Guide for Imaging
16.2 Defining an Optimal Input File Strategy for Oracle WebCenter Content: Imaging

The input file is the smallest unit of work that the input agent can schedule and process. There are multiple elements to be taken into consideration to achieve the highest performance, scalability, and high availability in an Imaging cluster:

- All of the machines in an Imaging cluster share a common input directory.
- Input files from this directory are distributed to each machine via a JMS queue.
- The frequency with which the directory is polled for new files is configurable.
- Each machine has multiple parsing agents that process the input files. The number of parsing agents is configured via the Work Manager created within the Oracle WebCenter Content: Imaging deployment.

Optimum performance will be achieved when:

- Each Imaging cluster instance has the maximum affordable number of parsing agents configured via the Work Manager without compromising the performance of the other Imaging activities, such as the user interface and Web services.
- The inbound flow of documents is partitioned into input files containing the appropriate number of documents. On average there should be two input files queued for every parsing agent within the cluster.
- If one or more machines within a cluster fails, active machines will continue processing the input files. Input files from a failed machine will remain in limbo until the server is restarted. Smaller input files ensure that machine failures do not place large numbers of documents into this limbo state.

For example, consider 10,000 inbound documents per hour being processed by two servers. A configuration of two parsing agents per server produces acceptable overall performance and ingests two documents per second per agent. The four parsing agents at two documents per second is eight documents per second, or 28,800 documents per hour. Note that a single input file of 10,000 documents will not be processed in an hour since a single parsing agent working at 7,200 documents per hour will be unable to complete it. However, if you divide the single input file up into eight input files of 1,250 documents, this ensures that all four parsing agents are fully utilized, and the 10,000 documents are completed in the one hour period. Also, if a failure should occur in one of the servers, the other can continue processing the work remaining on its parsing agents until the work is successfully completed.

16.3 Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology

When deploying SOA composites to the Oracle SOA Suite subsystem used by Oracle WebCenter Content: Imaging, deploy to a specific server’s address and not to the load balancer address (wcc.mycompany.com). Deploying to the load balancer address may require direct connection from the deployer nodes to the external load balancer address, which may require additional ports to be opened in the firewalls used by the system.
16.4 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. Watch for generic errors, such as oracle.fabric.common.FabricInvocationException, in the Oracle Enterprise Manager Fusion Middleware Control console (dashboard for instances). Search also in the Oracle SOA Suite server’s logs for errors, such as:

```
ORA-01691: unable to extend lob segment
SOAINFRA.SYS_LOB0000108469C00017$S$ 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. Additionally, old composite instances can be purged to reduce the SOA infrastructure database size. Oracle does not recommend using Oracle Enterprise Manager Fusion Middleware Control for this type of operation as in most cases the operations cause a transaction timeout.

Refer to "Managing SOA Composite Applications" in the Oracle Fusion Middleware Administrator’s Guide for Oracle SOA Suite for more details on the possible operations included in the SQL packages provided. 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.

16.5 Configuring UMS Drivers for Oracle WebCenter Content: Imaging

**Note:** This step is required only if the Oracle SOA Suite system used by Oracle WebCenter Content: Imaging is using Unified Messaging System (UMS).

UMS driver configuration is not automatically propagated in an Oracle SOA Suite cluster. When UMS is used by the Oracle SOA Suite system that Oracle WebCenter Content: Imaging invokes, this implies that you need to do the following:

1. Apply the configuration of UMS drivers in each and every one of the servers in the EDG topology that is using the driver.
2. When server migration is used, servers are moved to a different node's domain directory. It is necessary to pre-create the UMS driver configuration in the failover node. The UMS driver configuration file location is:

   ```
   ORACLE_BASE/admin/domain_name/mserver/domain_name/servers/server_name/tmp/_WL_user/ums_driver_name/*/configuration/driverconfig.xml
   ```

   (where **"** represents a directory whose name is randomly generated by Oracle WebLogic Server during deployment, for example, 3682yq).
To create the file in preparation for possible failovers, users can force a server migration and copy the file from the source node. For example:

1. Configure the driver for WLS_IMG1 in SOAHOST1.
2. Force a failover of WLS_IMG1 to SOAHOST2. Verify the directory structure for the UMS driver configuration in the failover node:

   \[ cd \text{ORACLE}\_\text{BASE}/\text{admin/}\text{domain}\_\text{name/}\text{mserver/}\text{domain}\_\text{name/}\text{servers/}\text{server}\_\text{name/}\text{tmp/}\_\text{WL}\_\text{user/}\text{ums}\_\text{driver}\_\text{name/}*/\text{configuration} \]

   (where * represents a directory whose name is randomly generated by WLS during deployment, for example, \text{3682yq}).

3. Run the following command on SOAHOST1 to do a remote copy of the driver configuration file from SOAHOST1 to SOAHOST2:

   \[ \text{scp ORACLE}\_\text{BASE/}\text{admin/}\text{domain}\_\text{name/}\text{mserver/}\text{domain}\_\text{name/}\text{servers/}\text{server}\_\text{name/}\text{tmp/}\_\text{WL}\_\text{user/}\text{ums}\_\text{driver}\_\text{name/}*/\text{configuration/driverconfig.xml oracle@SOAHOST2:ORACLE}\_\text{BASE/}\text{admin/}\text{domain}\_\text{name/}\text{mserver/}\text{domain}\_\text{name/}\text{servers/}\text{server}\_\text{name/}\text{tmp/}\_\text{WL}\_\text{user/}\text{ums}\_\text{driver}\_\text{name/}*/\text{configuration/} \]

   (where * represents a directory whose name is randomly generated by Oracle WebLogic Server during deployment, for example, \text{3682yq}).

It is required to restart the driver for these changes to take effect (that is, for the driver to consume the modified configuration):

1. Log in to the Oracle WebLogic Administration console.
2. Expand the environment node on the navigation tree.
3. Click Deployments.
4. Select the driver.
5. Click Stop and then **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 and then **Servicing all requests** and confirm the operation.

Make sure that you verify in Oracle Enterprise Manager Fusion Middleware Control that the properties for the driver have been preserved.

### 16.6 Scaling Up the Oracle WebCenter Content Topology

When you scale up the topology, you add new managed servers to nodes that are already running on one or more managed servers. You already have a node that runs a managed server that is configured with the necessary components. The node contains a WebLogic Server home and an Oracle Fusion Middleware home in shared storage. Use these existing 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 binaries at a new location or to run pack and unpack.
The scale-up procedure depends on the topology component:

- Section 16.6.1, "Scale-Up Procedure for Oracle WebCenter Content"
- Section 16.6.2, "Scale-Up Procedure for Oracle WebCenter Content: Imaging"
- Section 16.6.3, "Scale-Up Procedure for Oracle SOA Suite"

16.6.1 Scale-Up Procedure for Oracle WebCenter Content

Only one Oracle WebCenter Content managed server per node per domain is supported by Oracle Fusion Middleware. To add additional Oracle WebCenter Content managed servers, follow the steps in Section 16.7.1, "Scale-Out Procedure for Oracle WebCenter Content" to add an Oracle WebCenter Content managed server to a new node.

16.6.2 Scale-Up Procedure for Oracle WebCenter Content: Imaging

To scale up the Imaging servers in the enterprise deployment topology:

1. Using the Oracle WebLogic Server Administration Console, clone WLS_IMG1 to 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 Domain Structure window of the WebLogic Server Administration Console, expand the Environment node and then Servers.
   b. On the Summary of Servers page, click Lock & Edit and then select the managed server that you want to clone (WLS_IMG1).
   c. Click Clone.
   d. Name the new managed server WLS_IMGn, where n is a number that identifies the new managed server.
   e. For the server listen address, assign the host name or IP to use for this new managed server. If you are planning to use server migration for this server (which Oracle recommends), this should be the virtual host name for the server. This virtual host name should be different from the one used for the existing managed server.
   f. For the server listen port, enter the listening port number for the Imaging cluster (IMG_Cluster). The reference topology in this book uses port number 16000.
   g. Click OK and Activate Changes. You should now see the newly created server WLS_IMGn in the summary of servers.

The remainder of the steps that follow assume that you are adding a new server to WCCHOST1, which is already running WLS_IMG1.

Note: A shared domain directory for a managed server with Content Server does not work because certain files within the domain, such as intradoc.cfg, are specific to each node. To prevent issues with node-specific files, use a local (per node) domain directory for each Oracle WebCenter Content and Oracle WebCenter Content: Inbound Refinery managed server.
2. Configure a JMS persistence store and JMS servers for Oracle WebCenter Content: Imaging JMS.

Configure the location for the JMS persistence stores as a directory that is visible from both nodes. By default, the JMS servers used by Oracle WebCenter Content: Imaging are configured with no persistent store and use WebLogic Server’s store (ORACLE_BASE/admin/domain_name/mserver/domain_name/servers/server_name/data/store/default). You must change Oracle’s JMS server persistent store to use a shared base directory as follows:

a. Log in to the WebLogic Server Administration Console.
b. In the Domain Structure window, expand the Services node and then click the Persistence Stores node.
c. On the Summary of Persistence Stores page, click Lock & Edit.
d. Click New, and then Create FileStore.
e. On the Create a New File Store page, enter the following information:
   - Name: IMGJMServer\$ (for example, IMGJMServer3Store, which allows you identify the service it is created for)
   - Target: WLS_IMG\$ (for example, WLS_IMG3).
   - Directory: Specify a directory that is located in shared storage so that it is accessible from both WCCHOST1 and WCCHOST2 (ORACLE_BASE/admin/domain_name/img_cluster_name/jms).

   **Note:** This directory must exist before the managed server is started or the start operation will fail.

f. Click OK and activate the changes.

g. In the Domain Structure window, expand the Services node, then the Messages node, and then click JMS Servers.

h. On the Summary of JMS Servers page, click New and then enter the following information:
   - Name: IpmJmsServer\$ (for example, IpmJmsServer3)
   - Persistent Store: select the persistence store that you created above: IMGJMServer\$Store (for example, IMGJMServer3Store).

   Click Next and then specify WLS_IMG\$ (for example, WLS_IMG3) as the target. Click Finish and activate the changes.

i. Click the IpmJmsServer3 JMS server (represented as a hyperlink) in the Name column of the table.

j. On the settings page for the JMS server, click Lock & Edit.
**k.** In the Persistent Store drop-down list, select IMGJMSStore.

**l.** Click **Save** and activate the changes.

3. Configure a default persistence store for WLS_IMGn for transaction recovery:
   a. Log in to the WebLogic Server Administration Console.
   b. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.
   c. On the Summary of Servers page, click WLS_IMGn (represented as a hyperlink) in the Name column of the table. The settings page for the WLS_IMGn server opens with the **Configuration** tab active.
   d. Open the **Services** tab.
   e. Click **Lock & Edit**.
   f. 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/img_cluster_name/tlogs
   ```

   **Note:** This directory must exist before the managed server is started or the start operation will fail.

   g. Click **Save** and activate the changes.

4. Disable host name verification for the new managed server. Before you can start and verify the WLS_IMGn managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Administration Server and Node Manager in WCCHOSTn. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

To disable host name verification:
   a. In the Oracle Enterprise Manager console, select WebLogic Server Administration Console, and log in.
   b. In the Domain Structure window, expand the **Environment** node and click **Servers**.
   c. On the Summary of Servers page, click WLS_IMGn (represented as a hyperlink) in the Name column of the table. The settings page for the WLS_IMGn server opens with the **Configuration** tab active.
   d. Open the **SSL** tab.
   e. Expand the **Advanced** section of the page.
   f. Click **Lock & Edit**.
   g. Set host name verification to **None**.
   h. Click **Save**.
5. Start the newly created managed server (WLS_IMG):
   a. Log in to the WebLogic Server Administration Console.
   b. In the Domain Structure window, expand the **Environment** node and then click **Servers**.
   c. On the Summary of Servers page, open the **Control** tab, and shut down all existing WLS_IMG managed servers in the cluster.
   d. Ensure that the newly created managed server, WLS_IMGn, is running.

6. Add the host name of the WLS_IMGn managed server (WCCHOSTnVHN1) to the **SocketHostNameSecurityFilter** parameter list:
   a. Open the file `ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/config/config.cfg` in a text editor.
   b. Add the WLS_IMGn managed server to include listen addresses to the list of addresses that are allowed to connect to Oracle WebCenter Content:
      
      ```
      SocketHostNameSecurityFilter=localhost=localhost.mycompany.com|WCCHOST1|WCCHOST2|WCCHOST1VHN1|WCCHOST1VHN2|WCCHOST2VHN1
      ```
   c. Save the modified config.cfg file and restart the Oracle WebCenter Content servers for the changes to take effect.

7. Configure server migration for the new managed server.

   **Note:** Since this is a scale-up operation, the node should already contain a Node Manager and environment configured for server migration. The floating IP for the new managed Imaging server should also be already present.

To configure server migration:

   a. Log in to the WebLogic Server Administration Console.
   b. In the Domain Structure window, expand the **Environment** node and then click **Servers**.
   c. On the Summary of Servers page, click the name of the new managed server (represented as a hyperlink) in Name column of the table for which you want to configure migration.
   d. On the settings page for the selected server, open the Migration subtab.
   e. In the Migration Configuration section, select the servers that participate in migration in the **Available** window and click 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 WCCHOST1, which is already running WLS_IMG1, select WCCHOST2. For new managed servers on WCCHOST2, which is already running WLS_IMG2, select WCCHOST1.

   **Note:** The appropriate resources must be available to run the managed servers concurrently during migration.

   f. Choose the **Automatic Server Migration Enabled** option. This enables Node Manager to start a failed server on the target node automatically.
g. Click Save.

h. Restart the Administration Server, managed servers, and Node Manager.

8. Test server migration for the new server. To test migration, perform the following steps from the node where you added the new server:

- Abruptly stop the WLS_IMGn 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 the following command:
  
  ```bash
  ps -ef | grep WLS_IMGn
  ```
  
- Watch the Node Manager Console for a message indicating that WLS_IMGn's floating IP has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_IMGn. Node Manager waits for a fence period of 30 seconds before trying this restart.

- Once Node Manager restarts the server, stop it again. Node Manager should log a message indicating that the server will not be restarted again locally.

Note: After a server is migrated, to fail it back to its original node or machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.

16.6.3 Scale-Up Procedure for Oracle SOA Suite

To scale up the Oracle SOA Suite servers in the enterprise deployment topology:

Note: To scale up the Oracle SOA Suite subsystem used by Oracle WebCenter Content: Imaging, refer to the Oracle SOA Suite enterprise deployment topology documentation.

1. Using the WebLogic Server Administration Console, clone WLS_SOA1 to 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 Domain Structure window of the WebLogic Server Administration Console, expand the Environment node and then Servers.

b. On the Summary of Servers page, select the managed server that you want to clone (WLS_SOA1).

c. Click Clone.

d. Name the new managed server WLS_SOAn, where n is a number that identifies the new managed server.

Note: The remainder of the steps assume that you are adding a new server to SOAHOST1, which is already running WLS_SOAI.
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 for this server (which Oracle recommends), this should be the VIP (also called a floating IP) to enable it to move to another node. The VIP should be different from the one used by the managed server that is already running.

3. Create JMS servers for Oracle SOA Suite and UMS on the new managed server:
   a. Use the WebLogic Server Administration Console to create a new persistent store for the new SOA JMS Server and name it, for example, SOAJMSFileStore_N. Specify the path for the store. This should be a directory on shared storage, as recommended in Section 4.3, "Recommended Locations for the Different Directories":

   \[ \text{ORACLE}\_\text{BASE/admin/domain_name/soa\_cluster\_name/jms} \]

   **Note:** This directory must exist before the managed server is started or the start operation fails.

   b. Create a new JMS server for Oracle SOA Suite (for example, SOAJMSFileStore_N). Use the SOAJMSFileStore_N for this JMS server. Target the SOAJMSFileStore_N server to the recently created managed server (WLS_SOA\_n).

   c. Create a new persistence store for the new UMS JMS Server (for example, UMSJMSFileStore_N). Specify the path for the store. This should be a directory on shared storage, as recommended in Section 4.3, "Recommended Locations for the Different Directories":

   \[ \text{ORACLE}\_\text{BASE/admin/domain_name/soa\_cluster\_name/jms} \]

   **Note:** This directory must exist before the managed server is started or the start operation fails. You can also 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, UMSJMSFileStore_N). Use the UMSJMSFileStore_N for this JMS server. Target the UMSJMSFileStore_N server to the recently created managed server (WLS\_SOA\_n).

   e. Update the subdeployment targets for the SOA JMS Module to include the recently created SOA JMS server. To do this, expand the Services node in the WebLogic Server Administration Console and then expand the Messaging node. Choose JMS Modules in the Domain Structure window. The JMS Modules page appears. Click SOAJMSModule (represented as a hyperlink in the Names column of the table). The Settings page for SOAJMSModule appears. Open the SubDeployments tab. The subdeployment module for SOAJMS appears.

   **Note:** This subdeployment module name is a random name in the form of SOAJMS\_ServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS\_SOA1 and WLS\_SOA2).
Click the **SOAJMSServerXXXXXX** subdeployment. Add the new JMS server for Oracle SOA Suite called **SOAJMSServer_N** to this subdeployment. Click **Save**.

**f.** Update the subdeployment targets for the **UMSJMSSystemResource** to include the recently created UMS JMS server. To do this, expand the **Services** node in the WebLogic Server Administration Console and then expand the **Messaging** node. Choose **JMS Modules** in the Domain Structure window. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for **UMSJMSSystemResource** appears. Open the **SubDeployments** tab. The subdeployment module for UMSJMS appears.

---

**Note:** This subdeployment module name is a random name in the form of **UCMJMSServerXXXXXX** resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

---

Click the **UMSJMSServerXXXXXX** subdeployment. Add the new JMS server for UMS called **UMSJMSServer_N** to this subdeployment. Click **Save**.

4. **Configure 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
```

---

5. **Configure a TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage (see Section 4.3, "Recommended Locations for the Different Directories").**

From the Administration Console, select the server name (WLS_SOA{n}) in 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:

```
ORACLE_BASE/admin/domain_name(soa_cluster_name)/tlogs
```

6. **Disable host name verification for the new managed server. Before you can start and verify 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 Administration Server and Node Manager in SOAHOSTn. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).**

To disable host name verification:

**a.** In the Oracle Enterprise Manager console, select WebLogic Server Administration Console, and log in.

**b.** Expand the **Environment** node in the Domain Structure window.

**c.** Click **Servers**.
d. On the Summary or Servers page, select WLS_SOAn in the Names column of the table.

e. On the settings page for the server, open the SSL tab.

f. Expand the Advanced section of the page.

g. Click Lock & Edit.

h. Set host name verification to None.

i. Click Save.

7. Start and test the new managed server from the WebLogic Server Administration Console:

a. Ensure that the newly created managed server, WLS_SOAn, is running.

b. Access the application on the LBR (http://soainternal.mycompany.com/soa-infra). The application should be functional.

---

**Note:** The Oracle HTTP Servers in the topology should round-robin requests to the new added server (a few requests, depending on the number of servers in the cluster, may be required to hit the new server). Its 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 will take place only if at least one of the servers listed in the WebLogicCluster directive is running.

---

8. Configure server migration for the new managed server.

---

**Note:** Since this is a scale-up operation, the node should already contain a Node Manager and environment configured for server migration. The floating IP for the new Oracle SOA Suite managed server should also be already present.

---

To configure server migration:

a. Log in to the WebLogic Server Administration Console.

b. In the Domain Structure window, expand the Environment node and then click Servers.

c. On the Summary of Servers page, click the name of the new managed server (represented as a hyperlink) in Name column of the table for which you want to configure migration.

d. On the settings page for the selected server, open the Migration subtab.

e. In the Migration Configuration section, select the servers that participate in migration in the Available window and click 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.
Choose the **Automatic Server Migration Enabled** option. This enables Node Manager to start a failed server on the target node automatically.

Click **Save**.

Restart the Administration Server, managed servers, and Node Manager.

Test server migration for the new server. To test migration, perform the following steps from the node where you added the new server:

- Abruptly stop the WLS_SOA\textsubscript{n} 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 the following command:
  
  ```
  ps -ef | grep WLS_SOA\textsubscript{n}
  ```

- Watch the Node Manager Console for a message indicating that WLS\_SOA\textsubscript{1}'s floating IP has been disabled.

- Wait for Node Manager to attempt a second restart of WLS\_SOA\textsubscript{n}. Node Manager waits for a fence period of 30 seconds before trying this restart.

- Once Node Manager restarts the server, stop it again. Node Manager should log a message indicating that the server will not be restarted again locally.

---

**Note**: After a server is migrated, to fail it back to its original node or machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.

---

### 16.7 Scaling Out the Oracle WebCenter Content Topology

When scaling out the topology, you add new managed servers configured to new nodes.

**Prerequisites**

Before performing the steps in this section, check that you meet these requirements:

- There must be existing nodes running managed servers configured with Oracle Fusion Middleware within the topology.

- The new node can access the existing home directories for WebLogic Server and Fusion Middleware. (Use the existing installations in shared storage for creating a new managed server. You do not need to install WebLogic Server or Fusion Middleware 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, it is recommended that you 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 `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. See the following steps.

- The new server can use a new individual domain directory or, if the other managed servers domain directories reside on shared storage, reuse the domain directories on those servers.

---

**Note:** A shared domain directory for a managed server with Content Server does not work because certain files within the domain, such as intradoc.cfg, are specific to each node. To prevent issues with node-specific files, use a local (per node) domain directory for each Oracle WebCenter Content and Oracle WebCenter Content: Inbound Refinery managed server.

The scale-out procedure depends on the topology component:

- Section 16.7.1, "Scale-Out Procedure for Oracle WebCenter Content"
- Section 16.7.2, "Scale-Out Procedure for Oracle WebCenter Content: Imaging"
- Section 16.7.3, "Scale-Out Procedure for Oracle SOA Suite"

### 16.7.1 Scale-Out Procedure for Oracle WebCenter Content

To scale out the Oracle WebCenter Content servers in the enterprise deployment topology:

---

**Note:** These steps assume that you are adding a new WebCenter Content server to node n, where no managed server was running previously.

1. On the new node, mount the existing Middleware home, which should include the Oracle WebCenter Content installation and 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 on WCCHOSTn:
   
   ```bash
   cd ORACLE_COMMON_HOME/oui/bin/
   ./attachHome.sh -jreLoc ORACLE_BASE/product/fmw/jrockit_160_version
   ```

   To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the MW_HOME/bea/beahomelist file and add ORACLE_BASE/product/fmw 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 address to map the IP of the node that is being used for scale-out.

6. Use the WebLogic Server Administration Console to clone WLS_WCC1 into a new managed server. Name it WLS_WCCn, where n is a number.
7. Assign the host name or IP of WCCHOST\textsuperscript{n} to use for the new managed server as the listen address of the managed server.

8. Run the \texttt{pack} command on SOAHOST\textsuperscript{1} to create a template pack:

```
    cd ORACLE_COMMON_HOME/common/bin
    ./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name -template=edgdomaintemplateScaleWCC.jar -template_name=edgdomain_templateScaleWCC
```

9. Run the following command on SOAHOST\textsuperscript{1} to copy the created template file to WCCHOST\textsuperscript{n}:

```
    scp edgdomaintemplateScaleWCC.jar oracle@WCCHOST\textsuperscript{n}:/ORACLE_COMMON_HOME/common/bin
```

10. Run the \texttt{unpack} command on WCCHOST\textsuperscript{n} to unpack the template in the managed server domain directory:

```
    cd ORACLE_COMMON_HOME/common/bin
    ./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template=edgdomaintemplateScaleWCC.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

11. Start Node Manager on the new node if it has not started already. To start Node Manager, use the installation in shared storage from the already existing nodes and then start Node Manager by passing the host name of the new node as a parameter as follows (on WCCHOST\textsuperscript{n}):

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

12. Disable host name verification for the new managed server. Before you can start and verify the WLS_WCC\textsuperscript{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 Administration Server and Node Manager in WCCHOST\textsuperscript{n}. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification setting is propagated to the cloned server).
To disable host name verification:

a. In the Oracle Enterprise Manager console, select Oracle WebLogic Server Administration Console.
b. Expand the Environment node in the Domain Structure window.
c. Click Servers.
d. On the Summary of Servers page, select WLS_WCC\(n\) in the Names column of the table.
e. On the settings page for the server, open the SSL tab.
f. Expand the Advanced section of the page.
g. Click Lock & Edit.
h. Set host name verification to None.
i. Click Save.

13. Start the new managed server, WLS_WCC\(n\), from the WebLogic Server Administration Console:

a. Expand the Environment node in the Domain Structure window.
b. Choose Servers.
c. On the Summary of Server page, open the Control tab.
d. Select the WLS_WCC\(n\) server and then click Start.
e. Verify that the server status is reported as Running in the Administration Console.

14. Configure the new managed server, WLS_WCC\(n\):

a. Log in to WLS_WCC\(n\) at http://WCCHOST\(n\):16200/cs using your Oracle WebLogic Server administration user name and password. The WebCenter Content Configuration page opens.

**Note:** At the end of page you should see this text: Since the Revisions table in the database is not empty, you are not able to configure this server as a new instance. You may only configure this server to be a node in an existing cluster.

b. Change the following values on the server configuration page. Make sure that Cluster Node Identifier is set to match your managed server ID, such as WLS_WCC\(n\), and that the Is new Content Server Instance? checkbox is not selected.

* **Content Server Instance Folder:** Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs.

* **Native File Repository Location:** Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/vault.

* **WebLayout Folder:** Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/weblayout.

* **User Profile:** Set this to ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/data/users/profiles
c. Click **Submit** when finished and restart the new managed server using the WebLogic Server Administration Console.

15. Test the WLS_WCC\textsubscript{n} managed server by accessing the application on the LBR (https://wcc.mycompany.com/cs). The application should be functional.

---

**Notes:**

- The HTTP Servers in the topology should round-robin requests to the new 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 will take place only if at least one of the servers listed in the WebLogicCluster directive is running.

- If the scale-out procedure has been done to add a new WebCenter Content managed server, make sure that this newly added WCCHOST\textsubscript{n} is added to the list of servers in the Content Server pool while you create a connection to Oracle WebCenter Content. The servers to be added in the Content Server pool follow:

  - WCCHOST1:4444
  - WCCHOST2:4444
  - WCCHOST3:4444

  For more information, see Section 11.16, "Creating a Connection to Oracle WebCenter Content."

---

### 16.7.2 Scale-Out Procedure for Oracle WebCenter Content: Imaging

To scale out the Imaging servers in the enterprise deployment topology:

1. On the new node, mount the existing Middleware home, which should include the Oracle WebCenter Content installation and (optionally, if the domain directory for managed servers in other nodes resides on shared storage) 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 on WCCHOST\textsubscript{n}:

   ```bash
cd ORACLE_COMMON_HOME/oui/bin/
./attachHome.sh -jreLoc ORACLE_BASE/product/jrockit_160_version
```

   To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME/bea/beahomelist` file and add `ORACLE_BASE/product/fmw` 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 address to map the IP of the node that is being used for scale-out.
6. Use the WebLogic Server Administration Console to clone WLS_IMG1 into a new managed server. Name it WLS_IMGn, 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.

   **Note:** You must enable a VIP on node n, and you must also correctly resolve the host names in the network system used by the topology (either by DNS server or host resolution). To enable the VIPs, follow the example described in Section 9.2, “Enabling SOAHOST1VHN1 on SOAHOST1 and SOAHOST2VHN1 on SOAHOST2.”

   Also, assign the newly created server to the machine you added in the step 4. Without this, the machine name of the cloned server will remain.

8. Create a JMS server for Oracle WebCenter Content: Imaging on the new managed server:

   a. Use the WebLogic Server Administration Console to first create a new persistent store for the new IMGJMSServer (which will be created in a later step) and name it, for example, IMGJMSFileStore_N. Specify the path for the store as recommended in Section 4.3, “Recommended Locations for the Different Directories” as the directory for the JMS persistent stores:
      
      \( \text{ORACLE\_BASE/admin/domain\_name/cluster\_name/jms/} \)

   **Note:** This directory must exist before the managed server is started or the start operation will fail.

   b. Create a new JMS server for; for example, IMGJMSServer_N. Use the IMGJMSFileStore_N created above for this JMS server. Target the IMGJMSServer_N server to the recently created managed server (WLS_IMGn).

9. Run the `pack` command on SOAHOST1 to create a template pack:

   **Note:** If the domain directory for other managed servers resides on a shared directory, this step is not required. Instead, the new nodes mount the already existing domain directory and use it for the newly added managed server.

   ```
   cd ORACLE\_COMMON\_HOME/common/bin
   
   ./pack.sh -managed=true -domain=ORACLE\_BASE/admin/domain\_name/aserver/domain\_name -template=edgdomaintemplateScaleIMG.jar -template_name=edgdomain_templateScaleIMG
   ```
10. Run the following command on SOAHOST1 to copy the created template file to WCCHOSTn:

```
scp edgdomaintemplateScaleIMG.jar oracle@WCCHOSTn:/ORACLE_COMMON_HOME/common/bin
```

**Note:** If the new host, WCCHOSTn or SOAHOSTn, will use the same MW_HOME as SOAHOST1, then this step is not required.

11. Run the `unpack` command on WCCHOSTn to unpack the template in the managed server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template= edgdomaintemplateScaleIMG.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

12. Disable host name verification for the new managed server. Before you can start and verify the WLS_IMGn managed server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Administration Server and Node Manager in WCCHOSTn. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification setting is propagated to the cloned server).

To disable host name verification:

a. In the Oracle Enterprise Manager console, select **Oracle WebLogic Server Administration Console**.

b. Expand the **Environment** node in the Domain Structure window.

c. Click **Servers**.

d. On the Summary of Servers page, select WLS_IMGn in the Names column of the table.

e. On the settings page for the server, open the **SSL** tab.

f. Expand the **Advanced** section of the page.

g. Click **Lock & Edit**.

h. Set host name verification to **None**.

i. Click **Save**.

13. Start Node Manager on the new node. To start Node Manager, use the installation in shared storage from the already existing nodes and then start Node Manager by passing the host name of the new node as a parameter as follows (on WCCHOSTn):

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

**Note:** If you used the paths shown in Chapter 6.3.1, "Installing Oracle WebLogic Server and Creating the Middleware Home," WL_HOME would be ORACLE_BASE/product/fmw/wlservcer_10.3.
14. Start the new managed server, WLS_IMGn, from the WebLogic Server Administration Console and make sure it is running.

15. Add the new Imaging server listen addresses to the list of allowed hosts in Oracle WebCenter Content Server. Follow the steps in Section 11.15, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content" to add the new server to the SocketHostNameSecurityFilter configuration for Oracle WebCenter Content.

16. Restart all Oracle WebCenter Content managed servers.

---

**Note:** Make sure that the host names of all Imaging managed servers have been added to the SocketHostNameSecurityFilter parameter list in the ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/config/config.cfg file.

---

17. Test the WLS_IMGn managed server by accessing the application on the LBR (https://wcc.mycompany.com/imaging). The application should be functional.

---

**Note:** The HTTP Servers in the topology should round-robin requests to the new 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 will take place only if at least one of the servers listed in the WebLogicCluster directive is running.

---

18. Configure server migration for the newly added server.

---

**Note:** Since 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, and so on. Verify the privileges defined in the new node to make sure server migration will work. Refer to Chapter 14, "Configuring Server Migration for an Enterprise Deployment" for more details on privilege requirements.

---

To configure server migration:

a. Log in to the WebLogic Server Administration Console.

b. In the Domain Structure window, expand the Environment node and then click Servers.

c. On the Summary of Servers page, click the name of the server (represented as a hyperlink) in the Name column of the table for which you want to configure migration.

d. On the settings page for the selected server, open the Migration subtab.

e. In the Available field of the Migration Configuration section, select the machines to which to allow migration and click the right arrow.
Choose the **Automatic Server Migration Enabled** option. This enables Node Manager to start a failed server on the target node automatically.

Click **Save**.

Restart the Administration Server, managed servers, and Node Manager.

**19.** Test server migration for the new server. To test migration, perform the following steps from the node where you added the new server:

- Abruptly stop the WLS_IMGn 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 the following command:
  
  ```
  ps -ef | grep WLS_IMGn
  ```

- Watch the Node Manager Console for a message indicating that WLS_IMGn's floating IP has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_IMGn. Node Manager waits for a fence period of 30 seconds before trying this restart.

- Once Node Manager restarts the server, stop it again. Node Manager should log a message indicating that the server will not be restarted again locally.

---

**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.

---

**Note:** After a server is migrated, to fail it back to its original node or machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.
16.7.3 Scale-Out Procedure for Oracle SOA Suite

To scale out the Oracle SOA Suite servers in the topology:

---

**Note:** To scale out the Oracle SOA Suite subsystem used by Oracle WebCenter Content: Imaging, refer to the Oracle SOA Suite enterprise deployment topology documentation.

---

1. On the new node, mount the existing Middleware home, which should include the Oracle SOA Suite installation and 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 on SOAHOSTn:

   ```
   cd ORACLE_COMMON_HOME/oui/bin/
   ./attachHome.sh -jreLoc ORACLE_BASE/product/fmw/jrockit_160_version
   ```

   To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME/bea/beahomelist` file and add `ORACLE_BASE/product/fmw` 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 address to map the IP of the node that is being used for scale-out.

6. Use the WebLogic Server Administration Console to clone WLS_SOA1 into a new managed server. Name it WLS_SOA$n$, 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. Run the `pack` command on SOAHOST1 to create a template pack:

   ```
   cd ORACLE_COMMON_HOME/common/bin
   ./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name -template=edgdomaintemplateScaleSOA.jar -template_name=edgdomain_templateScaleSOA
   ```

---
9. Run the following command on SOAHOST1 to copy the created template file to SOAHOSTn:

```
scp edgdomaintemplateScaleSOA.jar oracle@SOAHOSTn:/ORACLE_COMMON_HOME/common/bin
```

10. Run the `unpack` command on SOAHOSTn to unpack the template in the managed server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=edgdomaintemplateScaleSOA.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

11. Create JMS servers for Oracle SOA Suite and UMS on the new managed server:

   a. Use the WebLogic Server Administration Console to create a new persistent store for the new SOAJMSServer and name it, for example, SOAJMSFileStore_N. Specify the path for the store. This should be a directory on shared storage as recommended in Section 4.3, "Recommended Locations for the Different Directories":

   
   ORACLE_BASE/admin/domain_name/cluster_name/jms

   **Note:** This directory must exist before the managed server is started or the start operation fails.

   b. Create a new JMS server for Oracle SOA Suite (for example, SOAJMSServer_N). Use SOAJMSFileStore_N for this JMS server. Target the SOAJMSServer_N server to the recently created managed server (WLS_SOA_n).

   c. Create a new persistence store for the new UMSJMServer (for example, UMSJMSFileStore_N). Specify the path for the store. This should be a directory on shared storage as recommended in Section 4.3, "Recommended Locations for the Different Directories":

   ORACLE_BASE/admin/domain_name/cluster_name/jms

   **Note:** This directory must exist before the managed server is started or the start operation fails. You can also 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_SOA_n).

   e. Update the subdeployment targets for the SOA JMS Module to include the recently created SOA JMS server. To do this, expand the Services node in the WebLogic Server Administration Console and then expand the Messaging node. Choose JMS Modules in the Domain Structure window. The JMS Modules page appears. Click SOAJMSModule (represented as a hyperlink in the Names column of the table). The Settings page for SOAJMSModule appears. Open the SubDeployments tab. The subdeployment module for SOA JMS appears.
Click the SOAJMSServerXXXXXX subdeployment. Add the new JMS server for Oracle SOA Suite called SOAJMSServer_N to this subdeployment. Click Save.

f. Update the subdeployment targets for the UMSJMSSystemResource to include the recently created UMS JMS server. To do this, expand the Services node in the WebLogic Server Administration Console and then expand the Messaging node. Choose JMS Modules in the Domain Structure window. The JMS Modules page appears. Click UMSJMSSystemResource (represented as a hyperlink in the Names column of the table). The Settings page for UMSJMSSystemResource appears. Open the SubDeployments tab. The subdeployment module for UMSJMS appears.

Note: This subdeployment module name is a random name in the form of SOAJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the SOAJMSServerXXXXXX subdeployment. Add the new JMS server for Oracle SOA Suite called SOAJMSServer_N to this subdeployment. Click Save.

Note: This subdeployment module name is a random name in the form of UCMJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the UMSJMSServerXXXXXX subdeployment. Add the new JMS server for UMS called UMSJMSServer_N to this subdeployment. Click Save.

12. Configure a TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage (see Section 4.3, "Recommended Locations for the Different Directories").

From the Administration Console, select the server name (WLS_SOAn) in 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:

```
ORACLE_BASE/admin/domain_name/soa_cluster_name/tlogs
```

13. Disable host name verification for the new managed server. Before you can start and verify 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 Administration Server and Node Manager in SOAHOSTn. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification setting is propagated to the cloned server).

To disable host name verification:

a. In the Oracle Enterprise Manager console, select Oracle WebLogic Server Administration Console.

b. Expand the Environment node in the Domain Structure window.

c. Click Servers.

d. On the Summary of Servers page, select WLS_SOAn in the Names column of the table.

e. On the settings page for the server, open the SSL tab.
f. Expand the Advanced section of the page.

g. Click Lock & Edit.

h. Set host name verification to None.

i. Click Save.

14. Start Node Manager on the new node. To start Node Manager, use the installation in shared storage from the already existing nodes and then start Node Manager by passing the host name of the new node as a parameter as follows (on SOAHOSTn):

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

**Note:** If you used the paths shown in Chapter 6.3.1, "Installing Oracle WebLogic Server and Creating the Middleware Home," WL_HOME would be ORACLE_BASE/product/fmw/wlserver_10.3.

15. Start the new managed server, WLS_SOAn, from the WebLogic Server Administration Console and make sure it is running.

16. Test the WLS_SOAn managed server by accessing the application on the LBR (http://soainternal.mycompany.com/soa-infra). The application should be functional.

**Note:** The HTTP Servers in the topology should round-robin requests to the new 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 will take place only if at least one of the servers listed in the WebLogicCluster directive is running.

17. Configure server migration for the newly added server.

**Note:** Since 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, and so on. The floating IP for the new Oracle SOA Suite managed server is already present in the new node.

To configure server migration:

a. Log in to the WebLogic Server Administration Console.

b. In the Domain Structure window, expand the Environment node and then click Servers.

c. On the Summary of Servers page, click the name of the server (represented as a hyperlink) in Name column of the table for which you want to configure migration.

d. On the settings page for the selected server, open the Migration subtab.
e. In the Available field of the Migration Configuration section, select the machines to which to allow migration and click the right arrow.

**Note:** Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional managed server.

e. Choose the Automatic Server Migration Enabled option. This enables Node Manager to start a failed server on the target node automatically.

g. Click Save.

h. Restart the Administration Server, managed servers, and Node Manager.

18. Test server migration for the new server. To test migration, perform the following steps from the node where you added the new server:

   - Abruptly stop the WLS_SOA 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 the following command:

     ```
     ps -ef | grep WLS_SOA
     ```

   - Watch the Node Manager Console for a message indicating that WLS_SOA's floating IP has been disabled.

   - Wait for Node Manager to attempt a second restart of WLS_SOA. Node Manager waits for a fence period of 30 seconds before trying this restart.

   - Once Node Manager restarts the server, stop it again. Node Manager should log a message indicating that the server will not be restarted again locally.

**Note:** After a server is migrated, to fail it back to its original node or machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.
Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments

Table 16–2 lists the static artifacts to back up in the Oracle WebCenter Content 11g enterprise deployment.

**Table 16–2 Static Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise Deployment**

<table>
<thead>
<tr>
<th>Type</th>
<th>Host</th>
<th>Location</th>
<th>Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORACLE HOME (DB)</td>
<td>CUSTDBHOST1 and</td>
<td>The location is user defined.</td>
<td>Data tier</td>
</tr>
<tr>
<td></td>
<td>CUSTDBHOST2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MW HOME (OHS)</td>
<td>WEBHOST1 and</td>
<td>ORACLE_BASE/product/fmw</td>
<td>Web tier</td>
</tr>
<tr>
<td></td>
<td>WEBHOST2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MW HOME (this includes the</td>
<td>SOAHOST1 and</td>
<td>MW_HOME</td>
<td>Application tier</td>
</tr>
<tr>
<td>SOA Oracle home as well)</td>
<td>SOAHOST2*</td>
<td>The SOA Oracle home is also under</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MW_HOME: ORACLE_HOME</td>
<td></td>
</tr>
<tr>
<td>Installation-related files</td>
<td></td>
<td>OraInventory, User_Home/bea/beahomelist,</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oraInst.loc, oratab</td>
<td></td>
</tr>
</tbody>
</table>

* WCCHOST1 and WCCHOST2 use the binaries installed from SOAHOST1 and SOAHOST2. Backup is centralized in SOAHOST1 and SOAHOST2.

Table 16–3 lists the runtime artifacts to back up in the Oracle WebCenter Content 11g enterprise deployment.

**Table 16–3 Runtime Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise Deployment**

<table>
<thead>
<tr>
<th>Type</th>
<th>Host</th>
<th>Location</th>
<th>Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application artifacts (EAR and WAR files)</td>
<td>SOAHOST1, SOAHOST2, WCCHOST1, and WCCHOST2</td>
<td>Find the application artifacts by viewing all of the deployments through the administration console.</td>
<td>Application tier</td>
</tr>
<tr>
<td>Oracle SOA Suite runtime artifacts</td>
<td>SOAHOST1 or SOAHOST2</td>
<td>ORACLE_BASE/admin/domain_name/soa_cluster_name</td>
<td>Application tier</td>
</tr>
<tr>
<td>Oracle WebCenter Content runtime artifacts</td>
<td>WCCHOST1 or WCCHOST2</td>
<td>ORACLE_BASE/admin/domain_name/wcc_cluster_name</td>
<td>Application tier</td>
</tr>
<tr>
<td>Oracle WebCenter Content: Imaging runtime artifacts</td>
<td>WCCHOST1 or WCCHOST2</td>
<td>ORACLE_BASE/admin/domain_name/img_cluster_name</td>
<td>Application tier</td>
</tr>
<tr>
<td>Customized managed server configuration for Oracle WebCenter Content</td>
<td>WCCHOST1 or WCCHOST2</td>
<td>ORACLE_BASE/admin/domain_name/mserver/domain_name/ucm/cs/bin/intradoc.cfg and ORACLE_BASE/admin/domain_name/mserver/domain_name/bin/server_migration/wlsifconfig.sh</td>
<td>Application tier</td>
</tr>
</tbody>
</table>
For more information on backup and recovery of Oracle Fusion Middleware components, see Oracle Fusion Middleware Administrator's Guide.

**16.9 Preventing Timeouts for SQLNet Connections**

Much of the production enterprise deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall to not time out such connections. If such a configuration is not possible, set the `*SQLNET.EXPIRE_TIME=n*` parameter in the `ORACLE_HOME/network/admin/sqlnet.ora` file on the database server, where `n` is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

**16.10 Configuring Oracle Web Service Manager Security Policies for Oracle WebCenter Content and Imaging Services**

When first installed, the Oracle WebCenter Content and Imaging web services are configured with no Oracle Web Service Manager (OWSM) security policies applied. When no security policies are applied, the services leverage the basic HTTP authentication mechanism, where user credentials (user ID and password) are transmitted in the web service HTTP message header. Oracle recommends using the appropriate Oracle WSM policy enforcements instead of basic HTTP authentication. To configure Oracle WSM security policies for Oracle WebCenter Content and Imaging web services, follow the steps in the Oracle WebCenter Content Developer's Guide for Imaging and the Oracle WebCenter Content Installation Guide.

<table>
<thead>
<tr>
<th>Type</th>
<th>Host</th>
<th>Location</th>
<th>Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customized managed server configuration</td>
<td>SOAHOST1 or SOAHOST2</td>
<td>If using UMS: <code>DOMAIN_HOME/servers/server_name/tmp/_WL_user/ums_driver_name/*/configuration/driverconfig.xml</code> (where * represents a directory whose name is randomly generated by WLS during deployment, for example, 3682yq) and <code>ORACLE_BASE/admin/domain_name/nservlet/domain_name/bin/server_migration/wlsifconfig.sh</code></td>
<td>Application tier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle HTTP Server instance home</td>
<td>WEBHOST1 and WEBHOST2</td>
<td><code>ORACLE_BASE/admin/instance_name</code></td>
<td>Web tier</td>
</tr>
<tr>
<td>Oracle RAC databases</td>
<td>CUSTDBHOST1 and CUSTDBHOST2</td>
<td>The location is user-defined.</td>
<td>Data tier</td>
</tr>
</tbody>
</table>

Table 16–3 (Cont.) Runtime Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise
16.11 Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology

This section covers the following topics:

- Section 16.11.1, "Page Not Found When Accessing soa-infra Application Through Load Balancer"
- Section 16.11.2, "Soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence)"
- Section 16.11.3, "Incomplete Policy Migration After Failed Restart of SOA Server"
- Section 16.11.4, "SOA, Oracle WebCenter Content, or Imaging Servers Fail to Start Due to Maximum Number of Processes Available in Database"
- Section 16.11.5, "Administration Server Fails to Start After a Manual Failover"
- Section 16.11.6, "Error While Activating Changes in Administration Console"
- Section 16.11.7, "SOA or Imaging Server Not Failed Over After Server Migration"
- Section 16.11.8, "SOA or Imaging Server Not Reachable From Browser After Server Migration"
- Section 16.11.9, "OAM Configuration Tool Does Not Remove URLs"
- Section 16.11.10, "Redirecting of Users to Login Screen After Activating Changes in Administration Console"
- Section 16.11.11, "Redirecting of Users to Administration Console’s Home Page After Activating Changes to OAM"
- Section 16.11.12, "Configured JOC Port Already in Use"
- Section 16.11.13, "Using CredentialAccessPermissions to Allow Oracle WebCenter Content: Imaging to Read Credentials From the Credential Store"
- Section 16.11.14, "Improving Performance with Very Intensive Document Uploads from Oracle WebCenter Content: Imaging to Oracle WebCenter Content"
- Section 16.11.15, "Out-of-Memory Issues on Managed Servers"
- Section 16.11.16, "Regenerating the Master Password for Oracle WebCenter Content Servers"
- Section 16.11.17, "Logging Out from the WebLogic Server Administration Console Does Not End the User Session"

16.11.1 Page Not Found When Accessing soa-infra Application Through Load Balancer

**Problem:** A 404 page not found message is displayed in the web browser when you try to access the soa-infra application using the load balancer address. The error is intermittent and Oracle SOA Suite servers appear as Running in the WebLogic Server Administration Console.

**Solution:** Even when the Oracle SOA Suite managed servers are up and running, some of the applications contained in them can be in Admin, Prepared or other states different from Active. The soa-infra application may be unavailable while the Oracle SOA Suite server is running. Check the Deployments page in the Administration Console to verify the status of the soa-infra application. It should be in the Active state. Check the Oracle SOA Suite server’s output log for errors pertaining to the soa-infra application and try to start it from the Deployments page in the Administration Console.
16.11.2 Soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence)

**Problem:** The soa-infra application fails to start after changes to the Coherence configuration for deployment have been applied. The Oracle SOA Suite server output log reports the following:

Cluster communication initialization failed. If you are using multicast, Please make sure multicast is enabled on your network and that there is no interference on the address in use. Please see the documentation for more details.

**Solutions:**

1. When using multicast instead of unicast for cluster deployments of SOA composites, you may get a message similar to the preceding one if a multicast conflict arises when starting the soa-infra application (that is, starting the managed server on which Oracle SOA Suite runs). These messages, which occur when Oracle Coherence throws a run-time exception, also include the details of the exception itself. If such a message appears, check the multicast configuration in your network. Verify that you can ping multicast addresses. In addition, check for other clusters that may have the same multicast address but have a different cluster name in your network, as this may cause a conflict that prevents soa-infra from starting. If multicast is not enabled in your network, you can change the deployment framework to use unicast as described in *Oracle Coherence Developer’s Guide for Oracle Coherence*.

2. When entering well-known address list for unicast (in server start parameters), make sure that the node’s addresses entered for the localhost and clustered servers are correct. Error messages like the following are reported in the server’s output log if any of the addresses is not resolved correctly:

   oracle.integration.platform.blocks.deploy.CompositeDeploymentCoordinatorMessage

16.11.3 Incomplete Policy Migration After Failed Restart of SOA Server

**Problem:** The Oracle SOA Suite server fails to start through the administration console before setting Node Manager property `startScriptEnabled=true`. The server does not come up after the property is set either. The Oracle SOA Suite server output log reports the following:

SEVERE: <.> Unable to Encrypt data
Unable to Encrypt data.
Check installation/post-installation steps for errors. Check for errors during SOA server startup.

ORABPEL-35010

Unable to Encrypt data.
Unable to Encrypt data.
Check installation/post-installation steps for errors. Check for errors during SOA server startup.

at oracle.bpm.services.common.util.EncryptionService.encrypt(EncryptionService.java:56)
...
**Solution:** Incomplete policy migration results from an unsuccessful start of the first Oracle SOA Suite server in a cluster. To enable full migration, edit the `<jazn-policy>` element in the system-jazn-data.xml file to grant permission to `bpm-services.jar`:

```xml
<grant>
  <grantee>
    <codesource>
      <url>file:${oracle.home}/soa/modules/oracle.soa.workflow_11.1.1/bpm-services.jar</url>
    </codesource>
  </grantee>
  <permissions>
    <permission>
      <class>java.security.AllPermission</class>
    </permission>
  </permissions>
</grant>
```

16.11.4 SOA, Oracle WebCenter Content, or Imaging Servers Fail to Start Due to Maximum Number of Processes Available in Database

**Problem:** An Oracle SOA Suite, Oracle WebCenter Content, or Imaging server fails to start. The domain has been extended for new types of managed server (for example, Oracle WebCenter Content extended for Imaging) or the system has been scaled up (added new servers of the same type). The Oracle SOA Suite, Oracle WebCenter Content, or Imaging server output log reports the following:

```xml
<Warning> <JDBC> <BEA-001129> <Received exception while creating connection for pool "SOADataSource-rac0": Listener refused the connection with the following error:
ORA-12516, TNS:listener could not find available handler with matching protocol stack >
```

**Solution:** Verify the number of processes in the database and adjust accordingly. As the SYS user, issue the SHOW PARAMETER command:

```
SHOW PARAMETER processes
```

Set the initialization parameter using the following SQL command:

```
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.
16.11.5 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:

<Feb 19, 2009 3:43:05 AM PST> <Warning> <EmbeddedLDAP> <BEA-171520> <Could not obtain an exclusive lock for directory: ORACLE_BASE/admin/edg_domain/aserver/edg_domain/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.lok.

16.11.6 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 Activate Changes is clicked:

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, provide user name and password information in the server start configuration in the Administration Console for the specific server whose configuration was being changed.

16.11.7 SOA or Imaging Server Not Failed Over After Server Migration

**Problem:** After reaching the maximum restart attempts by local Node Manager, Node Manager in the failover node tries to restart it, but the server does not come up. The server seems to be failed over as reported by Node Manager’s output information. The VIP used by the Oracle SOA Suite or Oracle WebCenter Content: Imaging server is not enabled in the failover node after Node Manager tries to migrate it (if config in the failover node does not report the VIP in any interface). Executing the command `sudo ifconfig $INTERFACE $ADDRESS $NETMASK` does not enable the IP in the failover node.

**Solution:** The rights and configuration for `sudo` execution should not prompt for a password. Verify the configuration of `sudo` with your system administrator so that `sudo` works without a password prompt.

16.11.8 SOA or Imaging Server Not Reachable From Browser After Server Migration

**Problem:** Server migration is working (Oracle SOA Suite or Oracle WebCenter Content: Imaging server is restarted in the failed over node), but the Virtual Hostname:8001/soa-infra URL cannot be accessed in the web browser. The server has been killed in its original host, and Node Manager in the failover node reports that the VIP has been migrated and the server started. The VIP used by the
Oracle SOA Suite or Imaging server cannot be pinged from the client's node (that is, the node where the browser is being used).

**Solution:** The `arping` command executed by Node Manager to update ARP caches did not broadcast the update properly. In this case, the node is not reachable to external nodes. Either update the nodemanager.properties file to include the MACBroadcast or execute a manual arping:

```
/sbin/arping -b -q -c 3 -A -I INTERFACE ADDRESS > $NullDevice 2>&1
```

Where `INTERFACE` is the network interface where the virtual IP is enabled and `ADDRESS` is the virtual IP address.

### 16.11.9 OAM Configuration Tool Does Not Remove URLs

**Problem:** The OAM Configuration Tool has been used and a set of URLs was added to the policies in Oracle Access Manager. One of multiple URLs had a typo. 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 in to the Access Administration site for OAM, click **My Policy Domains**, click the created policy domain (SOA_EDG), then click the **Resources** tab, and remove the incorrect URLs.

### 16.11.10 Redirecting of Users to Login Screen After Activating Changes in Administration Console

**Problem:** After configuring OHS and LBR to access the Oracle WebLogic Administration Console, some activation changes cause the redirection to the login screen for the Administration 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 `wcc.mycompany.com/console/console.portal` and directly access the home page for the Administration Console.

**Note:** This problem will not occur if you have disabled tracking of the changes described in this section.

### 16.11.11 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 the Administration Console is set to follow configuration changes (redirections are performed by the Administration Server when activating some changes). Activations should complete regardless of this redirection. For successive changes not to redirect, access the Administration Console, choose Preferences, then Shared Preferences, and unselect the **Follow Configuration Changes** checkbox.
16.11.12 Configured JOC Port Already in Use

**Problem:** Attempts to start a managed server that uses the Java Object Cache, such as OWSM 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.

16.11.13 Using CredentialAccessPermissions to Allow Oracle WebCenter Content: Imaging to Read Credentials From the Credential Store

**Problem:** Oracle WebCenter Content: Imaging creates the credential access permissions during startup and updates its local domain directory copy of the system-jazn-data.xml file. While testing the environment without an LDAP policy store being configured, the Administration Server may push manual updates to the system.jazn-data.xml file to the domain directories where the Oracle WebCenter Content: Imaging servers reside. This can cause the copy of the file to be overwritten, given rise to a variety of exceptions and errors in the restarts or access to the Oracle WebCenter Content: Imaging console.

**Solution:** To re-create the credential access permissions and update the Administration Server’s domain directory copy of the system-jazn-data.xml file, use the `grantIPMCredAccess` command from the Oracle WebLogic Scripting Tool. To do this, start `wlst.sh` from the ORACLE_HOME associated with Oracle WebCenter Content, connect to the Administration Server, and execute the `grantIPMCredAccess()` command on WCCHOST1:

```bash
cd ORACLE_HOME/common/bin
./wlst.sh
wls:/offline> connect()
wls:/domain_name/serverConfig> grantIPMCredAccess()
```

**Note:** When connecting, provide the credentials and address for the Administration Server.

16.11.14 Improving Performance with Very Intensive Document Uploads from Oracle WebCenter Content: Imaging to Oracle WebCenter Content

**Problem:** If a host name-based security filter is used in Oracle WebCenter Content (config.cfg file), a high latency and performance impact may be observed in the system in the event of very intensive document uploads from Oracle WebCenter Content: Imaging to Oracle WebCenter Content. This is caused by the reverse DNS lookup which is required in Oracle WebCenter Content to allow the connections from the Imaging servers.

**Solution:** Using a host name-based security filter is recommended in preparation of configuring the system for disaster protection and to restore to a different host (since the configuration used is IP-agnostic when using a host name-based security filter).
However, if the performance of the uploads needs to be improved, you can use an IP-based security filter instead of a host name-based filter.

To change the host name-based security filter in Oracle WebCenter Content to an IP-based filter:

1. Open the file `ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/config/config.cfg` in a text editor.

2. Remove or comment out the following two lines:

   ```
   SocketHostNameSecurityFilter=localhost|localhost.mycompany.com|wcchost1vhn1|wcchost2vhn1
   AlwaysReverseLookupForHost=Yes
   ```

3. Add the IP addresses (listen addresses) of the WLS_IMG1 and WLS_IMG2 managed servers (WCCHOST1VHN1 and WCCHOST2VHN1, respectively) to the `SocketHostAddressSecurityFilter` parameter list:

   ```
   SocketHostAddressSecurityFilter=127.0.0.1|0:0:0:0:0:0:0:1|X.X.X.X|Y.Y.Y.Y
   ```

   where X.X.X.X and Y.Y.Y.Y are the listen addresses of WLS_IMG1 and WLS_IMG2, respectively. (Please note that 127.0.0.1 must be included in the list as well.)

4. Save the modified config.cfg file and restart the Oracle WebCenter Content servers for the changes to take effect.

### 16.11.15 Out-of-Memory Issues on Managed Servers

**Problem:** You are experiencing out-of-memory issues on managed servers.

**Solution:** Increase the size of the memory heap allocated for the Java VM to at least one gigabyte:

1. Log in to the Oracle WebLogic Administration Console.

2. Click **Environment**, then **Servers**.

3. Click a managed server name.

4. Open the **Configuration** tab.

5. Open the **Server Start** tab in the second row of tabs.

6. Include the memory parameters in the Arguments box, for example:

   ```
   -Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m
   -XX:MaxPermSize=1024m
   ```

   **Note:** Please note that the memory parameter requirements may differ between various JVMs (Sun, JRockit, or others). See "Increasing the Java VM Heap Size for Managed Servers" in the *Oracle WebCenter Content Installation Guide* for further details.

7. Save the configuration changes.

8. Restart all running managed servers.
16.11.16 Regenerating the Master Password for Oracle WebCenter Content Servers

In case the cwallet.sso file of the Oracle WebCenter Content managed servers domain home becomes inconsistent across the cluster, is deleted, or is accidentally overwritten by an invalid copy in the ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig directory, you can perform these steps to regenerate the file:

1. Stop all Oracle WebCenter Content managed servers (WLS_WCCx).
2. Remove the cwallet.sso file from ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig.
3. Remove the password.hda file from ORACLE_BASE/admin/domain_name/aserver/wcc_cluster_name/cs/config/private.
4. Start the WLS_WCC1 server in WCCHOST1.
5. Verify the creation or update of the cwallet.sso file in ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig as well as the creation of the password.hda file in ORACLE_BASE/admin/domain_name/aserver/wcc_cluster_name/cs/config/private.
6. Use Oracle WebCenter Content’s System Properties command-line tool to update the passwords for the database.
7. Verify that the standalone Oracle WebCenter Content applications (Batchloader, System Properties, and so on) are working correctly.
8. Copy the cwallet.sso file from ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig to the Administration Server's domain directory at ORACLE_BASE/admin/domain_name/aserver/domain_name/config/fmwconfig.
9. Start the second Oracle WebCenter Content server, and verify that the Administration Server pushes the updated cwallet.sso file to ORACLE_BASE/admin/domain_name/mserver/domain_name/config/fmwconfig in WCCHOST2 and that the file is the same as created or updated by the Oracle WebCenter Content server in WCCHOST1.
10. Verify that the standalone Oracle WebCenter Content applications (Batchloader, System Properties, and so on) are working correctly.
11. Verify that the standalone Oracle WebCenter Content applications work correctly on both nodes at the same time.

16.11.17 Logging Out from the WebLogic Server Administration Console Does Not End the User Session

When you log in to the WebLogic Server administration console using Oracle Access Manager single sign-on (SSO), then clicking the logout button does not end the user session. You are not redirected to the OAM login page, which is in accordance with the SSO logout guidelines, but rather the home page is reloaded. To truly log out, you may need to manually clean up the cookies for your web browser.
Oracle recommends using GridLink data sources when developing new Oracle RAC applications. However, if you are using legacy applications and databases that do not support GridLink data sources, refer to the information in this appendix.

This appendix provides the following topics:

- Section A.1, "About Multi Data Sources and Oracle RAC"
- Section A.2, "Typical Procedure for Configuring Multi Data Sources for an EDG Topology"

A.1 About Multi Data Sources and Oracle RAC

A multi data source provides an ordered list of data sources to use to satisfy connection requests. Normally, every connection request to this kind of multi data source is served by the first data source in the list. If a database connection test fails and the connection cannot be replaced, or if the data source is suspended, a connection is sought sequentially from the next data source on the list.

For more information about configuring Multi Data Sources with Oracle RAC, see "Using Multi Data Sources with Oracle RAC" in the Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server.

A.2 Typical Procedure for Configuring Multi Data Sources for an EDG Topology

You configure data sources when you configure a domain. For example, when you are configuring the initial Administration domain for an Enterprise Deployment reference topology, you use the configuration wizard to define the characteristics of the domain, as well as the data sources.

The procedures for configuring the topologies in this Enterprise Deployment Guide include specific instructions for defining GridLink data sources with Oracle RAC. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the following:

1. In the Configure JDBC Component Schema screen:
   a. Select the appropriate schemas.
   b. For the RAC configuration for component schemas, Convert to RAC multi data source.
c. Ensure that the following data source appears on the screen with the schema prefix when you ran the Repository Creation Utility.

d. Click Next.

2. The Configure RAC Multi Data Sources Component Schema screen appears (Figure A–1).

**Figure A–1 Configure RAC Multi Data Source Component Schema Screen**

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.
   
   - **Username:** Enter the complete user name for the database schema owner of the corresponding component.

   This book uses *DEV* as the prefix of user names for the database 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.

3. In the Test JDBC Data Sources screen, the connections are 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.
access files for OAM, 15-35
access gate, 15-16
access servers, 15-19
adapters
  enabling high availability for Oracle File Adapter, 9-26
  enabling high availability for Oracle FTP Adapter, 9-26
  scaling Oracle Database Adapter, 9-29
address security filter, 10-18, 11-20, 12-10, 16-35
admin role, 15-7
admin users and groups, 15-6
admin.conf, 8-9
Administration Console
  creating domain, 8-1
  error when activating changes, 16-33
  redirecting to home page, 16-34
  redirecting to login screen, 16-34
Administration Server, 14-5
  application directory location, 4-6
  backing up the domain, 8-14
  boot.properties on SOAHOST1, 8-5
  configuring Oracle HTTP Server for --, 8-9
  creating domain with --, 8-3
  cwallet file, 10-19, 16-37
  disabling host name verification, 8-8
  enabling ADMINVHN on SOAHOST1, 8-2
  failing over to SOAHOST1, 8-14
  failing over to SOAHOST2, 8-12
  listen address, 8-4
  listen port, 8-4
  port, 3-8
  restarting, 10-17, 11-17, 12-9
  setting frontend URL, 8-11
  start failure, 16-33
  starting on SOAHOST1, 8-7
  validation, 8-8
admin.mycompany.com, 3-2
ADMINVHN, 3-5
  enabling -- on SOAHOST1, 8-2
agent for WebGate, 15-30
application tier, 2-4, 4-3
artifacts, 16-3
associating Inbound Refinery servers with virtual hosts, 12-2
associating Oracle web tier with WebLogic domain, 7-3
attachHome.sh script, 4-2
attributes of OID, 15-11
authentication scheme, 15-34
authenticator
  LDAP, 15-4
  OID, 15-4
  OVD, 15-4
authenticators, 15-25, 15-35
authorization scheme, 15-16, 15-34
backup
  after creating domain with Admin Server, 8-14
  after extending domain with Oracle SOA Suite, 9-30
  after extending domain with Oracle WebCenter Content, 10-24
  after extending domain with Oracle WebCenter Content: Imaging, 11-25
  after installing Oracle Fusion Middleware, 6-9
  after loading metadata repository into database, 5-10
  after setting up Oracle HTTP Server, 6-4
backups
  configuration files, 15-25, 15-35
  domain, 9-3
  enterprise deployments, 16-28
  installation, 15-37
basic cookieless scheme for Oracle Access Manager 11g, 15-35
best practices
  timeouts for SQLNet connections, 16-29
boot.properties for Administration Server, 8-5, 15-8
BPEL CSF credentials, 11-21
cataloging OID attributes, 15-11
certificates
  host name verification, 13-2
  self-signed, 13-3
clock synchronization, 2-6
cluster agent, 1-4
cluster communication, 2-5
clusters
  frontend HTTP host and port, 9-24, 11-23
  sharing master passwords between nodes, 10-19, 16-37
clusterware, 1-4
composites, 9-11, 16-3
configuration
  BPEL CSF credentials, 11-21
  creating domain, 8-1
  credential store, 15-3
  custom keystores for Node Manager, 13-5
  database, 5-2
  default JMS persistence store for Oracle WebCenter Content: Imaging, 11-15
  default persistence store, 9-25, 11-16
  delegated form authentication, 15-19
  environment variables, 4-1
  extending domain with Inbound Refinery, 12-1
  extending domain with Oracle SOA Suite components, 9-1
  extending domain with Oracle WebCenter Content, 10-1
  extending domain with Oracle WebCenter Content: Imaging, 11-1
  frontend HTTP host and port, 9-24, 11-23
  frontend URL for Administration Console, 8-11
  GDFontPath MBean, 11-18
  input directories for imaging, 11-18
  IP validation, 15-24
  Java Object Cache, 9-20
  JOC port in use, 16-35
  LDAP, 3-9
  load balancer, 3-2
  Node Manager, 13-1
  Node Manager for WLS_IMG managed servers, 10-23, 11-24
  Node Manager for WLS_SOA managed servers, 9-30
  Node Manager for WLS_WCC managed servers, 10-23
  Oracle Coherence, 9-11
  Oracle HTTP Server, 7-3
  Oracle HTTP Server for Admin Server, 8-9
  Oracle HTTP Server for WLS_IMG managed servers, 11-23
  Oracle HTTP Server for WLS_SOA managed servers, 9-22
  Oracle HTTP Server for WLS_WCC managed servers, 10-22
  policy store, 15-3, 15-9
  propagating domain configuration, 9-19, 10-17, 11-15, 12-8
  sample directory for imaging, 11-18
  server migration, 14-1
  server migration for WLS_IMG managed servers, 11-24
  server migration for WLS_SOA managed servers, 9-30
  service retries for Oracle WebCenter Content, 10-21
  shared storage, 4-10
  targets for server migration, 14-7
  UMS drivers, 16-4
  virtual hosts, 7-3
  web tier, 7-1
  WebGate, 15-20
  WLS_WCC1 managed server, 10-18
  WLS_WCC2 managed server, 10-19
  workflow connection, 11-22
configuration MBeans, 11-18
Configuration Wizard
  creating domain with Admin Server, 8-3
  extending domain with Oracle SOA Suite components, 9-3
  extending domain with Oracle WebCenter Content, 10-3
  extending domain with Oracle WebCenter Content: Imaging, 11-4
  extending domain with Oracle WebCenter Content: Inbound Refinery, 12-3
Configure GridLink RAC Component Schema screen, 9-5, 10-6, 11-6
configure-joc.py, 9-20
connecting Imaging to Oracle WebCenter Content, 11-20
Content Server
  enabling Inbound Refinery components, 12-13
  conversion jobs, Inbound Refinery, setting up, 12-12
  cookieless scheme for Oracle Access Manager 11g, 15-35
createCentralInventory.sh script, 6-3, 6-6
creating domain, 8-1
creating Fusion Middleware home, 6-4
credential store, 3-9, 15-3, 15-9, 15-10, 16-35
CredentialAccessPermissions, 16-35
credentials for Oracle WebCenter Content: Imaging, 11-21
CSF credentials for Oracle WebCenter Content: Imaging, 11-21
CUSTDBHOST, 2-5, 5-7
custom keystores, 13-5, 13-6
cwallet.sso, 10-19, 16-37
D
data source, 14-3
data sources, A-2
data tier, 2-5, 5-2
database, 2-5
  backing up, 5-10
  components, 5-8
  connection, 5-7
  host requirements, 5-2
  initialization parameters, 5-3
  loading metadata repository, 5-6
maximum number of processes, 16-32
port, 3-8
prefix for schemas, 5-7
services, 5-3
setting up, 5-2
supported versions, 5-2
database listener port, 2-5
database mutex locking, 9-26
deploying composites, 9-11
deploying composites and artifacts, 16-3
directory environment variables, 4-1
directory structure, 4-2
application directory (admin server), 4-6
application directory (managed servers), 4-6
domain directory, 4-5
Imaging images, 4-5
Imaging input files, 4-5
Inbound Refinery, 4-6
JMS file stores, 4-5
MW_HOME, 4-3
Oracle WebCenter Content vault, 4-6
ORACLE_BASE, 4-3
ORACLE_COMMON_HOME, 4-4
ORACLE_HOME, 4-4
ORACLE_INSTANCE, 4-4
Tlogs, 4-5
WL_HOME, 4-4
disabling host name verification
Administration Server, 8-8
for WLS_IMG managed servers, 11-11
for WLS_SOA managed servers, 9-14
domain
backing up, 9-3
creating domain, 8-1
extending domain with Oracle SOA Suite components, 9-1
extending domain with Oracle WebCenter Content, 10-1, 12-1
extending domain with Oracle WebCenter Content: Imaging, 11-1
propagating domain configuration, 9-19, 10-17, 11-15, 12-8
domain configuration
propagating, 9-18
domain directory, 4-2
admin directory, 4-5
managed server directory, 4-5
domain policy store, 15-10

backups and recoveries, 16-28
benefits, 1-6
credential store, 3-9
directory structure, 4-2
environment variables, 4-1
high availability, 1-6
installing software, 6-1
LDAP, 3-9
overview, 1-1
policy store, 3-9
security, 1-6
software, 2-7
terminology, 1-3
topology, 2-1
environment privileges, 14-7
environment variables, 4-1
extending domain
Inbound Refinery, 12-1
Oracle SOA Suite components, 9-1
Oracle WebCenter Content, 10-1
Oracle WebCenter Content: Imaging, 11-1

failback, 1-3
failing over Admin Server to SOAHOST1, 8-14
failing over Admin Server to SOAHOST2, 8-12
failover, 1-3, 16-33
file formats, selecting for Inbound Refinery conversion, 12-13
firewalls, 3-6
FMW, see 'Oracle Fusion Middleware (FMW)'
frontend HTTP host and port, 9-24, 11-23
frontend URL for Administration Console, 8-11

GCC libraries, 15-27
GDFontPath MBean, 11-18
generating self-signed certificates, 13-3
GridLink data source, 14-3
configuring, 9-5, 10-6, 11-5
verifying configuration, 9-15, 10-14, 11-12
GridLink RAC component schema, 9-5, 10-6, 11-6

hardware requirements, 2-5
high availability, 1-6, 9-26
home page, redirecting to, 16-34
host identifier, 15-17
host name based security filter, 11-20
host name verification

certificates for Node Manager, 13-2
disabling -- for Admin Server, 8-8
disabling -- for WLS_IMG managed servers, 11-11
disabling -- for WLS_SOA managed servers, 9-14
managed servers, 13-7

ECM, see 'Oracle WebCenter Content'
enabling ADMINVHN on SOAHOST1, 8-2
enabling Imaging in Oracle WebCenter Content, 11-20
Enterprise Content Management, see 'Oracle WebCenter Content'
enterprise deployment

failback, 1-3
failing over Admin Server to SOAHOST1, 8-14
failing over Admin Server to SOAHOST2, 8-12
failover, 1-3, 16-33
file formats, selecting for Inbound Refinery conversion, 12-13
firewalls, 3-6
FMW, see 'Oracle Fusion Middleware (FMW)'
frontend HTTP host and port, 9-24, 11-23
frontend URL for Administration Console, 8-11

GCC libraries, 15-27
GDFontPath MBean, 11-18
generating self-signed certificates, 13-3
GridLink data source, 14-3
configuring, 9-5, 10-6, 11-5
verifying configuration, 9-15, 10-14, 11-12
GridLink RAC component schema, 9-5, 10-6, 11-6

hardware requirements, 2-5
high availability, 1-6, 9-26
home page, redirecting to, 16-34
host identifier, 15-17
host name based security filter, 11-20
host name verification

certificates for Node Manager, 13-2
disabling -- for Admin Server, 8-8
disabling -- for WLS_IMG managed servers, 11-11
disabling -- for WLS_SOA managed servers, 9-14
managed servers, 13-7
Index-4

host names
  network, 1-4
  Oracle Coherence, 9-12
  physical, 1-4
  virtual, 1-5

hosts
  database, 5-2
  httpd.conf, 7-4

I
  ID Asseter, 15-25, 15-36
  identity keystore, 13-4
  IDM, see ‘Oracle Identity Management (IDM)’
  Imaging, 1-2
  Inbound Refinery, 1-2
    associating with virtual hosts, 12-2
    configuration, 12-9
    Content Server, setting up jobs for conversion, 12-12
    conversion jobs
      from Content Server, 12-12
      setting up, 12-12
    directory location, 4-6
    enabling components on Content Server, 12-13
    extending the domain, 12-3
    outgoing provider from Content Server, 12-12
    selecting file formats for conversion, 12-13
    starting, 12-9
  incomplete policy migration, 16-31
  incorrect URLs, 16-34
  incremental enterprise deployment, 2-10
  infrastructure database for Oracle SOA Suite, 16-4
  initialization parameters for database, 5-3
  input directories for Oracle WebCenter Content:
    Imaging, 11-18
  input file strategy for Oracle WebCenter Content:
    Imaging, 16-3
  inspection.wsil, 15-34
  installation
    creating domain, 8-1
    extending domain with Oracle SOA Suite components, 9-1
    extending domain with Oracle WebCenter Content, 10-1, 12-1
    extending domain with Oracle WebCenter Content: Imaging, 11-1
    Fusion Middleware home, 6-4
    modular approach, 2-10
    Oracle Fusion Middleware, 6-4
    Oracle Fusion Middleware components, 6-5
    Oracle HTTP Server, 6-2
    Oracle WebCenter Content, 6-5, 6-8
    Oracle WebLogic Server, 6-4
    procedure, 2-7
    software, 6-1
    validating web tier, 7-3
    WebGate, 15-20, 15-27
  what to install, 2-7

integration
  Oracle Access Manager 10g, 15-12
  Oracle Access Manager 11g, 15-26
  IP validation, 15-24
  IP-based security filter, 16-35
  I/PM, see ‘Oracle WebCenter Content: Imaging’
  IPs
    physical, 1-5, 3-4
    virtual, 1-5, 3-4

J
  Java Object Cache, 9-20, 16-35
  Java VM, memory heap for --, 16-36
  JMS file stores
    location, 4-5
  JMS persistence store
    Oracle WebCenter Content: Imaging, 11-15
  JOC port, 16-35

K
  keystores
    custom, 13-5, 13-6
    identity, 13-4
    trust, 13-4
  keytool utility, 13-4

L
  LDAP, 3-9, 15-3
    assigning admin role to admin group, 15-7
    moving WebLogic Server administrator to, 15-6
    provisioning admin users and groups, 15-6
  LDAP authenticator, 15-4
  leasing table for server migration, 14-2
  leasing.ddl script, 14-3
  listen address
    Administration Server, 8-4
    Oracle WebCenter Content: Imaging, 11-20
    WLS_IMG managed servers, 11-9, 11-20
    WLS_SOA managed servers, 9-9
    WLS_WCC managed servers, 10-9, 12-4
  listen port
    Administration Server, 8-4
    WLS_IMG managed servers, 11-9
    WLS_SOA managed servers, 9-9
    WLS_WCC managed servers, 10-9, 12-4
  listener port, 2-5
  load balancer, 1-6
    configuration, 3-2
    configuring with Oracle HTTP Server, 7-3
    port, 3-7
    requirements, 2-3, 3-2
    virtual server, 3-3
  loading metadata repository into database, 5-6
  log file for Node Manager, 13-2
  login screen, redirecting to, 16-34
  logout guidelines for OAM, 15-15
  logout URL, 15-16
managed servers
  adding to existing nodes (Oracle SOA Suite), 16-10
  adding to existing nodes (Oracle WebCenter Content: Imaging), 16-6
  adding to existing nodes (WebCenter Content), 16-6
  adding to new nodes (Oracle SOA Suite), 16-23
  adding to new nodes (Oracle WebCenter Content), 16-15
  adding to new nodes (Oracle WebCenter Content: Imaging), 16-18
application directory location, 4-6
custom keystores, 13-6
disabling host name verification, 9-14, 11-11
host name verification, 13-7
memory heap for Java VM, 16-36
out-of-memory issues, 16-36
propagating domain changes, 9-18
WLS_IMG, 10-23, 11-9, 11-17, 11-23, 11-24
WLS_SOA, 9-9, 9-22, 9-30
WLS_WCC, 10-9, 10-22, 10-23, 12-4
managing space in SOA infrastructure database, 16-4
managing the topology, 16-1
manual failover, 16-33
mapping of virtual IPs, 3-5
master passwords, 10-19, 16-37
MBean
  config, 11-18
  GDFontPath, 11-18
memory heap for Java VM, 16-36
metadata repository, 5-6
Middleware home, 1-3
migration of policies, 16-31
migration of servers, see ‘server migration’, 14-1
monitoring the topology, 16-2
mounting shared storage locations, 4-10
mutex locking, 9-26
MW_HOME (application tier), 4-1, 4-3
MW_HOME (web tier), 4-1
Node Manager, 13-3, 14-5
  configuration for WLS_IMG managed servers, 10-23, 11-24
  configuration for WLS_SOA managed servers, 9-30
  configuration for WLS_WCC managed servers, 10-23
  custom keystores, 13-5
  host name verification certificates, 13-2
  identity keystore, 13-4
  listen address for Admin Server, 8-5
  listen address for SOAHOST, 9-10, 11-10
  listen address for WCCHOST, 10-11, 11-10, 12-6
  log file, 13-2
  port, 3-8
  properties file, 14-6
  setup, 13-1
  starting, 13-7
  starting on SOAHOST1, 8-6
  starting on SOAHOST2, 9-15
  starting on WCCHOST, 10-14, 11-12, 12-8
  trust keystore, 13-4
nodes
  adding servers to existing -- (Oracle SOA Suite), 16-10
  adding servers to existing -- (WebCenter Content), 16-6
  adding servers to existing -- (WebCenter Content: Imaging), 16-18
  primary, 1-4
  secondary, 1-4

native file repository location for Oracle WebCenter Content, 4-6

O
OAM, see ‘Oracle Access Manager (OAM)’
OAM11gRequest.xml, 15-31
OAMCFG tool
  collecting information, 15-13
  running, 15-14
OAMHOST, 2-3
oamreg tool, 15-33
OHS, see ‘Oracle HTTP Server (OHS)’
OID attributes, 15-11
OID authenticator, 15-4
Oracle Access Manager (OAM) 10g integration, 15-12
adding access servers, 15-19
collecting information for OAMCFG tool, 15-13
configuration, 15-13
delegated form authentication, 15-19
ID Asserter, 15-25
IP validation, 15-24
logout guidelines, 15-15
order of providers, 15-25

Index-5
overview, 15-12
prerequisites, 15-13
running OAMCFG tool, 15-14
setting up WebGate, 15-27
updating host identifier, 15-17
updating WebGate profile, 15-18
validation, 15-36
verifying access gate, 15-16
verifying policy domain, 15-16
verifying the authorization scheme, 15-16
WebGate, 15-20
WebLogic Server authenticators, 15-25
Oracle Access Manager (OAM) 11g
integration, 15-26
access files, 15-35
GCC libraries, 15-27
ID Asserter, 15-36
inspection.wsil, 15-34
installing WebGate, 15-27
oamreg tool, 15-33
overview, 15-26
prerequisites, 15-26
registering WebGate agent, 15-30
RREG tool, 15-30
updating OAM11gRequest file, 15-31
validation, 15-36
Oracle Access Manager 11g integration
basic cookieless scheme, 15-35
order of providers, 15-36
WebLogic Server authenticators, 15-35
Oracle BI EE
upgrade roadmap table, 2-9
Oracle Coherence, 9-11, 16-31
Oracle Common home, 1-3
Oracle Database Adapter, 9-29
Oracle File Adapter
enabling high availability for --, 9-26
Oracle FTP Adapter
enabling high availability for --, 9-26
Oracle Fusion Middleware (FMW)
backing up, 6-9
creating FMW home, 6-4
installing FMW components, 6-5
installing Oracle WebLogic Server, 6-4
installing software, 6-4
Oracle home, 1-3
Oracle HTTP Server (OHS), 2-3
backing up, 6-4
configuration, 7-3
configuring -- for Administration Server, 8-9
configuring -- for WLS_IMG managed servers, 11-23
configuring -- for WLS_SOA managed servers, 9-22
configuring -- for WLS_WCC managed servers, 10-22
installation, 6-2
load balancer, 3-3, 7-3
location, 6-3
port, 3-7, 6-2
registering -- with Oracle WebLogic Server, 8-10
validating Admin Server access, 8-12, 8-14
validating Oracle SOA Suite server access, 9-25
validating Oracle WebCenter Content server access, 10-22
validating Oracle WebCenter Content: Imaging server access, 11-24
validating SSO, 15-36
Oracle Identity Management (IDM)
overview, 2-3
Oracle instance, 1-3
Oracle Notification Service
configuring, 9-5, 10-6, 11-5
verifying configuration, 9-15, 10-14, 11-12
Oracle SOA Suite
backing up the domain, 9-30
extending domain with --, 9-1, 9-3
installation, 6-5
ports, 3-7
Oracle UCM, see ‘Oracle WebCenter Content’
Oracle Web Services Manager (WSM), 2-4, 9-20, 16-29
Oracle WebCenter Content, 1-2
backing up the domain, 10-24
creating Imaging connection, 11-20
enabling Imaging, 11-20
extending domain with --, 10-1, 10-3, 12-1
extending domain with Imaging, 11-4
extending domain with Inbound Refinery, 12-3
installation, 6-8
native file repository location, 4-6
ports, 3-7
security for web services, 16-29
service retries, 10-21
vault location, 4-6
Oracle WebCenter Content: Imaging, 1-2
adding Imaging server listen addresses to Oracle WebCenter Content security filter, 11-20
backing up the domain, 11-25
configuring BPEL CSF credentials, 11-21
configuring workflow connection, 11-22
creating connection to Oracle WebCenter Content, 11-20
enabling -- in Oracle WebCenter Content, 11-20
extending domain with --, 11-1
file locations, 4-5
IP-based security filter, 16-35
optimal input file strategy, 16-3
ports, 3-7
reading credentials from the credential store, 16-35
security for web services, 16-29
Oracle WebCenter Content: Inbound Refinery, 1-2
Oracle WebLogic Scripting Tool (WLST)
starting Administration Server, 8-7
Oracle WebLogic Server (WLS), 2-4
associating with Oracle web tier, 7-3
installation, 6-4
logging out, 16-37
registering Oracle HTTP Server with --, 8-10
Index-7

ORACLE_BASE, 4-1, 4-3
ORACLE_COMMON_HOME, 4-2, 4-4
ORACLE_HOME, 4-2, 4-4
ORACLE_HOME (web tier), 4-4
ORACLE_INSTANCE, 4-2, 4-4
oracleRoot.sh script, 6-3
outgoing provider from Content Server to Inbound
Refinery, 12-12
out-of-memory issues, 16-36
OVD authenticator, 15-4
parameters for database, 5-3
persistance store, 9-25, 11-16
Oracle WebCenter Content: Imaging, 11-15
physical host name, 1-4
physical IP, 1-5
policy domain, 15-16
policy migration, 16-31
policy store, 3-9, 15-3
configuration, 15-9
reassociating, 15-9, 15-10
reassociation, 15-10
ports, 3-6
Administration Server, 3-8
database, 3-8
frontend HTTP port, 9-24, 11-23
Imaging, 3-7
JOC port in use, 16-35
load balancer, 3-7
Node Manager, 3-8
Oracle HTTP Server, 3-7, 6-2
Oracle SOA Suite, 3-7
Oracle WebCenter Content, 3-7
prefix for database schemas, 5-7
primary node, 1-4
processes in database, 5-3, 16-32
propagating domain changes, 9-18
propagating domain configuration, 9-19, 10-17,
11-15, 12-8
properties file of Node Manager, 14-6
protected URLs, 15-31
provider order for OAM, 15-25
provider order for Oracle Access Manager, 15-36
Prefix for database schemas, 5-7
primary node, 1-4
processes in database, 5-3, 16-32
propagating domain changes, 9-18
propagating domain configuration, 9-19, 10-17,
11-15, 12-8
properties file of Node Manager, 14-6
protected URLs, 15-31
provider order for OAM, 15-25
provider order for Oracle Access Manager, 15-36
R
RAC database, 2-5, 5-6, A-2
RAC database, see also ‘database’
RCU, see ‘Repository Creation Utility (RCU)’
reassociating ~/. 15-9, 15-10
reassociating the credential store, 15-9, 15-10
reassociating the domain policy store, 15-10
reassociating the policy store, 15-9, 15-10
recovery of enterprise deployments, 16-28
redirecting to home page, 16-34
redirecting to login screen, 16-34
registering Oracle HTTP Server with WebLogic
Server, 8-10
registering the WebGate agent, 15-30
Repository Creation Utility (RCU), 5-1
loading FMW Utility (RCU), 5-6
requirements
cluster communication, 2-5
database host, 5-2
hardware, 2-5
load balancer, 2-3, 3-2
software, 2-7, 6-1
unicast communication, 2-5
restarting
Administration Server, 10-17, 11-17, 12-9
retries for Oracle WebCenter Content services, 10-21
RREG tool, 15-30
S
sample directory for Oracle WebCenter Content:
Imaging, 11-18
scaling out the topology, 16-14
Oracle SOA Suite, 16-23
Oracle WebCenter Content, 16-15
Oracle WebCenter Content: Imaging, 16-18
scaling the Oracle Database Adapter, 9-29
scaling up the topology, 16-5
Oracle SOA Suite, 16-10
Oracle WebCenter Content, 16-6
Oracle WebCenter Content: Imaging, 16-6
screens
Configure GridLink RAC Component
Schema, 9-5, 10-6, 11-6
scripts
attachHome.sh, 4-2
createCentralInventory.sh, 6-3, 6-6
 leasing.ddl, 14-3
oracleRoot.sh, 6-3
setNMProps.sh, 8-6
wlsifconfig.sh, 14-7
secondary node, 1-4
security, 1-6
security filter, 10-18, 11-20, 12-10, 16-35
security policies, 16-29
self-signed certificates, 13-3
server migration, 14-1
configuration for WLS_IMG managed
servers, 11-24
configuration for WLS_SOA managed
servers, 9-30
configuring targets, 14-7
creating a GridLink data source, 14-3
determining Node Manager’s properties file, 14-6
enabling SSL communication, 14-5
GridLink data source, 14-3
leasing table, 14-2
setting environment and superuser
privileges, 14-7
setting up user and tablespace, 14-2
testing, 14-8
troubleshooting, 16-33
service retries for Oracle WebCenter Content, 10-21
ServiceAllowRetry, 10-21
services for database, 5-3
setNMProps.sh script, 8-6
setting up Node Manager, 13-1
setting up WebLogic Server authenticators, 15-25, 15-35
shared storage, 1-4
  configuration, 4-10
diagram, 4-8, 4-9
  example configuration, 4-8, 4-9
mounting locations, 4-10
single sign-on validation, 15-36
SOA infrastructure database, 16-4
SOAHOST, 2-4
  boot.properties for Admin Server, 8-5
  creating domain with Admin Server, 8-3
  creating Fusion Middleware home, 6-4
  enabling ADMINVHN on --, 8-2
  enabling SOAHOSTnVHNn, 9-3
  extending domain with Imaging, 11-4
  extending domain with Inbound Refinery, 12-3
  extending domain with Oracle SOA Suite components, 9-3
  extending domain with Oracle WebCenter Content, 10-3
failing over Administration Server, 8-12, 8-14
installing Oracle SOA Suite, 6-5
installing Oracle WebLogic Server, 6-4
mounting shared storage locations, 4-10
propagating domain configuration, 9-19
starting Administration Server, 8-7
starting Node Manager, 8-6, 9-15
starting WLS_SOA managed server, 9-18, 9-20
SOAHOST1VHN1, 3-5
  enabling -- on SOAHOST1, 9-3
SOAHOST2VHN1, 3-5
  enabling -- on SOAHOST2, 9-3
soa-infra application, 16-30, 16-31
soainternal.mycompany.com, 3-2
software
  database, 5-2
  installation, 6-1
  Oracle Fusion Middleware, 6-4
  Oracle HTTP Server, 6-2
  Oracle WebLogic Server, 6-4
  requirements, 2-7, 6-1
  versions, 2-7, 6-1
space in SOA infrastructure database, 16-4
SQLNet connections, timeouts, 16-29
SSL communication, 14-5
SSO validation, 15-36
starting
  Administration Server on SOAHOST1, 8-7
  Node Manager, 13-7
  Node Manager on SOAHOST1, 8-6
  Node Manager on SOAHOST2, 9-15
  Node Manager on WCCHOST, 10-14, 11-12, 12-8
  Oracle WebCenter Content: Imaging, 11-17
  WLS_SOA1 managed server, 9-18
  WLS_SOA2 managed server, 9-20
  WLS_WCC1 managed server, 10-18
  WLS_WCC2 managed server, 10-19
  superuser privileges, 14-7
  switchback, 1-5
  switchover, 1-5
  synchronization of clocks, 2-6
  system MBeans for Oracle WebCenter Content:
    Imaging, 11-18
T
tablespace for server migration, 14-2
targets for server migration, 14-7
terminology, 1-3
testing of server migration, 14-8
timeouts for SQLNet connections, 16-29
Tlogs
  location, 4-5
topology, 2-1
  application tier, 2-4
  credential store, 3-9
  data tier, 2-5
  directory structure, 4-2
  environment variables, 4-1
  installing software, 6-1
  managing, 16-1
  monitoring, 16-2
  Oracle Identity Management (IDM), 2-3
  policy store, 3-9
  scaling out, 16-14
  scaling out (Oracle SOA Suite), 16-23
  scaling out (Oracle WebCenter Content), 16-15
  scaling out (Oracle WebCenter Content: Imaging), 16-18
  scaling up, 16-5
  scaling up (Oracle SOA Suite), 16-10
  scaling up (Oracle WebCenter Content), 16-6
  scaling up (Oracle WebCenter Content: Imaging), 16-6
  software, 2-7
  web tier, 2-3
transaction recovery, 9-25, 11-16
troubleshooting
  activating changes in Admin Server, 16-33
  Coherence, 16-31
  deployment framework issues (Coherence), 16-31
  incomplete policy migration, 16-31
  incorrect URLs, 16-34
  logging out of WLS admin console, 16-37
  manual failover, 16-33
  maximum number of processes in database, 16-32
  memory heap for Java VM, 16-36
  no access to soa-infra application through load balancer, 16-30
  out-of-memory issues, 16-36
  redirecting to home page, 16-34
  redirecting to login screen, 16-34
  regenerating master password for Oracle WebCenter Content servers, 16-37
security filter, 16-35
server migration, 16-33
soa-infra application, 16-30, 16-31
trust keystore, 13-4

U
UCM, see 'Oracle WebCenter Content'
UMS drivers, 16-4
unicast communication, 2-5, 9-11
updating the host identifier, 15-17
updating WebGate profile, 15-18
URLs, protected --, 15-31
utils.CertGen utility, 13-3
utils.ImportPrivateKey utility, 13-4

V
validation
Admin Server access through Oracle HTTP Server, 8-12, 8-14
Administration Server, 8-8
OAM integration, 15-36
Oracle SOA Suite server access through Oracle HTTP Server, 9-25
Oracle WebCenter Content server access through Oracle HTTP Server, 10-22
Oracle WebCenter Content: Imaging server access through Oracle HTTP Server, 11-24
server migration, 14-8
SSO through Oracle HTTP Server, 15-36
web tier installation, 7-3
WLS_SOA1 managed server, 9-18
WLS_SOA2 managed server, 9-20
vault location for Oracle WebCenter Content, 4-6
verifying the authorization scheme, 15-16
versions of software, 2-7, 6-1
database, 5-2
VIPs, see 'virtual IPs (VIPs)'
virtual host name, 1-5
virtual hosts
ADMINVHN, 3-5
configuration, 7-3
SOAHOST1VHN1, 3-5
SOAHOST2VHN1, 3-5
WCCHOST1VHN1, 3-5
WCCHOST2VHN1, 3-6
virtual IPs (VIPs), 1-5, 3-4
ADMINVHN, 8-2
description, 3-5
mapping, 3-5
SOAHOST1VHN1, 9-3
SOAHOST2VHN1, 9-3
VIP4 and VIP5, 11-4
WCCHOST1VHN1, 10-3
WCCHOST2VHN1, 10-3
virtual servers
admin.mycompany.com, 3-2
load balancer, 3-3
soainternal.mycompany.com, 3-2
wcinternal.mycompany.com, 3-2
wcc.mycompany.com, 3-2
<VirtualHost> entries in httpd.conf, 7-4

W
wccedg.mycompany.com, 5-3, 5-7
WCCHOST, 2-4
enabling VIP4 and VIP5, 11-4
enabling WCCHOSTnVHNn, 10-3
installing Oracle WebCenter Content, 6-8
propagating domain configuration, 10-17, 11-15, 12-8
starting Node Manager, 10-14, 11-12, 12-8
starting Oracle WebCenter Content: Imaging, 11-17
starting WLS_WCC managed server, 10-18, 10-19
WCCHOST1VHN1, 3-5
enabling -- on WCCHOST1, 10-3
WCCHOST2VHN1, 3-6
enabling -- on WCCHOST2, 10-3
wcinternal.mycompany.com, 3-2
wcc.mycompany.com, 3-2
web services, 16-29
web tier, 2-3, 4-4
associating with WebLogic domain, 7-3
configuration, 7-1
validating installation, 7-3
WebCenter Content, 1-2
WebCenter Content, see 'Oracle WebCenter Content'
WebGate, 2-3
configuration, 15-24
installation, 15-20, 15-27
registering agent, 15-30
setup, 15-27
WebGate profile, 15-18
WEBHOST, 2-3
admin.conf, 8-9
associating web tier with WebLogic domain, 7-3
configuring OHS with load balancer, 7-3
configuring Oracle HTTP Server for Admin Server, 8-9
configuring web tier, 7-2
installing Oracle HTTP Server, 6-3
load balancer, 3-3
registering Oracle HTTP Server with WebLogic Server, 8-10
validating Admin Server access through Oracle HTTP Server, 8-12, 8-14
validating Oracle SOA Suite server access through Oracle HTTP Server, 9-25
validating Oracle WebCenter Content server access through Oracle HTTP Server, 10-22

Index-9
validating Oracle WebCenter Content: Imaging server access through Oracle HTTP Server, 11-24
validating SSO through Oracle HTTP Server, 15-36
WebLogic plug-in enabled flag, 8-10
WebLogic Server administrator, moving to LDAP, 15-6
WebLogic Server authenticators, 15-25, 15-35
WebLogic Server home, 1-3
WebLogic Server, see ‘Oracle WebLogic Server (WLS)’
WL_HOME, 4-2, 4-4
WLS, see ‘Oracle WebLogic Server (WLS)’
WLS_IMG managed servers, 11-9
   adding listen addresses to Oracle WebCenter Content, 11-20
   configuring Node Manager, 10-23, 11-24
   configuring Oracle HTTP Server, 11-23
   configuring server migration, 11-24
   disabling host name verification, 11-11
   starting, 11-17
WLS_SOA managed servers, 9-9
   configuring Node Manager, 9-30
   configuring Oracle HTTP Server, 9-22
   configuring server migration, 9-30
   disabling host name verification, 9-14
   starting, 9-18, 9-20
WLS_WCC managed servers, 10-9, 12-4
   configuring Node Manager, 10-23
   configuring Oracle HTTP Server, 10-22
   starting, 10-18, 10-19
wlsifconfig.sh script, 14-7
workflow connection for Oracle WebCenter Content: Imaging, 11-22
WSM, see ‘Oracle Web Services Manager (WSM)’

X

XWindows environment, 11-18